IRREDUCIBILITY OVER THE RATIONALS

Edward Cass Traasdahl

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

IRREDUCIBILITY OVER THE RATIONALS

by

Edward Cass Traasdahl

September 1975

Thesis Advisor Daniel L. Davis

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) IRREDUCIBILITY OVER THE RATIONALS		5. TYPE OF REPORT & PERIOD COVERED Master's Thesis September 1975 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Edward Cass Traasdahl		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		12. REPORT DATE September 1975 13. NUMBER OF PAGES 79
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) Naval Postgraduate School Monterey, California 93940		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Irreducibility, Rationals

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

A brief historical survey indicates the type of general irreducibility criteria that are sufficient for irreducibility over the rationals. Three general approaches to the problem are then examined in turn. The first of these involves an application of ideal theory for number fields, the second a construction of Newton polygons for which an appropriate multiplication theorem holds and the last a method for constructing non-Archimedean values on the field of fractions of the ring of polynomials over the rationals

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601 |
(Page 1)

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

from which irreducibility criteria can be deduced.

The conclusion summarizes the nature of these attempts.

Irreducibility over the Rationals

by

Edward Cass Traasdahl
Captain, United States Marine Corps
B.A., University of California at Long Beach, 1967

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE WITH MAJOR IN MATHEMATICS

from the

NAVAL POSTGRADUATE SCHOOL
September 1975

ABSTRACT

A brief historical survey indicates the type of general irreducibility criteria that are sufficient for irreducibility over the rationals. Three general approaches to the problem are then examined in turn. The first of these involves an application of ideal theory for number fields, the second a construction of Newton polygons for which an appropriate multiplication theorem holds and the last a method for constructing non-Archimedean values on the field of fractions of the ring of polynomials over the rationals from which irreducibility criteria can be deduced.

The conclusion summarizes the nature of these attempts.

TABLE OF CONTENTS

TABLE OF SPECIAL SYMBOLS

Z	The integers
Z^+	The positive integers
Q	The Rationals
$Q[x]$	The ring of polynomials over the rationals
$Q(x)$	The field of fractions over $Q[x]$
(u,v)	The greatest common divisor of u and v
∎	Halmos symbol
R	The extended reals
$[a]$	The greatest integer less than or equal to a

ACKNOWLEDGEMENT

The author wishes to express his sincere appreciation of the guidance and assistance provided by Professor Daniel L. Davis in the research for and the preparation of this work.

1. INTRODUCTION

1.1 BACKGROUND

A polynomial is said to be *reducible over the rationals* if it is expressible as a product of polynomials over the rationals of positive degree. Otherwise it is said to be *irreducible*.

Kronecker [9] has shown that it is always possible, in a finite number of steps, to decompose a polynomial into a product of irreducible polynomials. However the calculations required by his method, even when a computer is used, are excessive in general [10].

The actual decomposition of a polynomial is frequently not as important as simply knowing whether a given polynomial is irreducible or not. The mathematical literature contains a large number of *irreducibility criteria* designed to answer this question. Unfortunately no single criteria applies to all classes of polynomials.

The most recent survey of the question is given by Dorwart [4] in 1935 who summarizes the results of a number of writers on the subject. He divides the irreducibility criteria into three classes: *(i)* those depending on the divisibility properties of the coefficients, *(ii)* those depending on the comparative size of the coefficients and *(iii)* those depending on arithmetical properties of the values of the polynomial for integral arguments.

This thesis will expand and extend the criteria of the first type.

1.2 BRIEF HISTORICAL SURVEY

The earliest irreducibility criterion is a theorem due to Schönemann [18].

1.2.1 *Theorem* (*Schönemann, 1846*)

Let $f(x) = \phi^m(x) + p\psi(x)$

where:

(i) $\phi(x)$ is an irreducible polynomial modulo p and of degree n

(ii) $\deg\psi < mn$

(iii) $\psi(x) \not\equiv 0 \pmod{p, \phi(x)}$,

then f(x) is irreducible.

The next and probably best known irreducibility criterion is due to Eisenstein [6].

1.2.2 *Theorem* (*Eisenstein, 1850*)

Let $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$

where:

(i) $a_i \equiv 0 \pmod{p}$ $(i = 1, 2, \ldots, n)$

(ii) $a_n \not\equiv 0 \pmod{p^2}$,

then f(x) is irreducible.

Eisenstein's Theorem is a particular case of Schönemann's Theorem for $\phi(x) \equiv x$ and $\psi(x) \equiv (f(x) - x^n)/p$.

The Schönemann-Eisenstein Theorem was generalized by Königsberger [8] and Netto [16].

1.2.3 *Theorem* (*Königsberger, 1895*)

Let $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$

where:

(i) $a_i = p^{[ie/n]+1}b_i$ $(i = 1, 2, \ldots, n-1)$ and e is an integer relatively prime to n.

(ii) $a_n = p^e b_n$ where $(b_n, p) = 1$,

then f(x) is irreducible.

Setting e = 1 we obtain Eisenstein's Theorem.

1.2.4 *Theorem* (*Netto, 1897*)

Let $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$

where:

(i) $a_i = pb_i \quad (i = 1, 2, \ldots, s-1)$

(ii) $a_i = p^2b_i \quad (i = s, s+1, \ldots, n)$

(iii) $b_n \not\equiv 0 \pmod{p}$

(iv) $n > 2s$,

then f(x) has no factors of degree less than s+1.

1.2.5 *Corollary I* If $n = 2s+2$, then f(x) can have only two irreducible factors each of degree s+1.

1.2.6 *Corollary II* If $n = 2s+1$ then f(x) is irreducible.

Later Königsberger's Theorem was generalized by Bauer [2] and Perron [17].

1.2.7 *Theorem* (*Bauer, 1905*)

Let $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$

where for s rational primes $p_1, p_2, \ldots, p_s$:

(i) $n = \prod_{k=1}^{s} n_k, \quad (n_i, n_j) = 1 \quad (1 \leq i < j \leq s)$

(ii) $a_i = \prod_{k=1}^{s} p_k^{[(ie_k-1)/n_k]+1} b_i$ where $e_k \in Z^+$ and $(e_k, n_k) = 1$

(iii) $(b_n, \prod_{k=1}^{s} p_k) = 1$,

then f(x) is irreducible.

1.2.8 *Theorem* (*Perron, 1905*)

Let $p_1, p_2, \ldots, p_s$ be rational primes. Then the polynomial

$$f(x) = x^n + \prod_{k=1}^{s} p_k^{[e_k/n]} + 1 a_1 x^{n-1} + \prod_{k=1}^{s} p_k^{[2e_k/n]} + 1 a_2 x^{n-2}$$

$$+ \ . \ . \ . \ + \prod_{k=1}^{s} p_k^{[(n-1)e_k/n]} + 1 a_{n-1} x + \prod_{k=1}^{s} p_k^{e_k} a_n$$

where:

(i) $a_i \in Z \qquad (i = 1, 2, \ldots, n)$

(ii) $(a_n, p_k) = 1 \ (k = 1, 2, \ldots, s)$

(iii) $(n, e_1, e_2, \ldots, e_s) = 1$,

is irreducible.

Bauer also generalized Schönemann's Theorem [3].

1.2.9 *Theorem (Bauer, 1905)*

Let $f(x) = \phi^{\alpha}(x) + p^{\beta}\psi(x)$

where:

(i) $\phi(x)$ is irreducible modulo p and of degree n

(ii) $(\alpha, \beta) = 1$

(iii) $\deg\psi < \alpha n$

(iv) $\psi(x) \not\equiv 0 \ (\mathrm{modd}\ p, \phi(x))$,

then f(x) is irreducible.

The following three sections examine the methods developed by Perron, Dumas and MacLane.

II. IDEAL THEORY AND IRREDUCIBILITY OVER THE RATIONALS

2.1 INTRODUCTION

In a finite extension $\mathbb{Q}[\xi]$ of $\mathbb{Q}$ a rational prime ideal (p) will factor as a product of prime ideals $\overline{\prod} P_i$. The way (p) factors may yield some information on the degree of $\mathbb{Q}[\xi]$ over $\mathbb{Q}$.

Dedekind [17] p. 449, proved the irreducibility of the p^{th} *cyclotomic polynomial* $(x^p-1)/(x-1)$ by showing that the rational prime ideal (p) in the field $\mathbb{Q}[\xi]$, where ξ is a p^{th} root of unity, was the $p-1^{st}$ power of a prime ideal which implies that $[\mathbb{Q}[\xi],\mathbb{Q}] \geq p-1$. Hence $(x^p-1)/(x-1)$ is irreducible.

O. Perron generalized this approach and then applied ideal theory to several irreducibility criteria. His method makes use of two well-known propositions [11] p. 63.

2.1.1 *Proposition I* A rational prime number can have at most n factors in an extension $\mathbb{Q}[\xi]$ of degree n over $\mathbb{Q}$.

2.1.2 *Proposition II* A rational prime number can be the e^{th} power of an ideal in an extension $\mathbb{Q}[\xi]$ of degree n over $\mathbb{Q}$ only if $e|n$.

2.2 APPLICATION OF PERRON'S METHOD TO EISENSTEIN'S CRITERIA

2.2.1 *Theorem (Eisenstein)*

Let $f(x) = x^n + pa_1x^{n-1} + \ldots + pa_n$

where $a_i \varepsilon Z$ and $(p,a_n) = 1$. Then $f(x)$ is irreducible.

Proof. Let $\mathbb{Q}[\zeta]$ be an extension of $\mathbb{Q}$ where $f(\zeta) = 0$. Then

$$(1) \qquad \zeta^n = -p(a_1\zeta^{n-1} + a_2\zeta^{n-2} + \ldots + a_n)$$

Let (ζ,p) be the gcd of ζ and p in $\mathbb{Q}[\zeta]$. Then $(\zeta,p) \neq 1$. For suppose this were the case. Then there would exist ideals S and T such that $S\zeta + Tp = 1$ which implies

$$(2) \qquad (S\zeta + Tp)^n = 1$$

Now p divides each term in the expansion of (2) since by (1) $p|\zeta^n$, thus $p|1$ which is a contradiction.

Reducing (1) still further we obtain

$$(3) \qquad \zeta^n/p = -(a_1\zeta^{n-2} + \ldots + a_{n-1}) - a_n$$

But (3) implies ζ^n/p is relatively prime to (ζ,p). For suppose not, then there exists an $\eta \neq 1$ such that $\eta|\zeta^n/p$, $\eta|\zeta$ and $\eta|p$. (3) then implies that $\eta|a_n$. Hence $\eta|(a_n,p)$ which is a contradiction since $(a_n,p) = 1$.

We also have $(\zeta,p)^n|\zeta^n$ which implies that $(\zeta,p)^n|p$. Since we have that $(\zeta,p)^n$ divides the right-hand-side of (1), if $(\zeta,p)^n$ does not divide p then some positive power of (ζ,p) would divide $(a_1\zeta^{n-1} + a_2\zeta^{n-2} + \ldots + a_n)$ and thus (ζ,p) would divide this expression also. But (ζ,p) divides every term up to the last a_n which implies that $(\zeta,p)|a_n$ but $(a_n,p) = 1$ and so we have a contradiction.

Now $(\zeta,p)^n = (\zeta^n,p^n)$ and $p|\zeta^n$ (from (1)) hence $p|(\zeta,p)^n$. Therefore $p = (\zeta,p)^n$. By propositions I and II we then have $[\mathbb{Q}[\zeta],\mathbb{Q}] = n$ and so $f(x)$ is irreducible.

∎

2.3 APPLICATION TO A THEOREM OF KONIGSBERGER

2.3.1 *Theorem* (*Königsberger*)

Let $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$

where:

(i) $a_i = p^{[ie/n] + 1}b_i \qquad (i=1, 2, \ldots, n-1)$

e a positive integer relatively prime to n,

(ii) $a_n = p^e b_n, \quad (p,b_n) = 1,$

then f(x) is irreducible.

Proof. Let $\mathbb{Q}\,\zeta$ be an extension of $\mathbb{Q}$ where $f(\zeta) = 0$.

Then, as in the previous theorem, we have that $p|\zeta^n$ and

ζ and p have a common ideal factor $\mathfrak{P} \neq 1$. Let

$\mathfrak{P}^a$ be the highest power of $\mathfrak{P}$ that divides p and

$\mathfrak{P}^b$ the highest power of $\mathfrak{P}$ that divides ζ. Then $\mathfrak{P}^{bn}$

is the highest power of $\mathfrak{P}$ that divides ζ^n and $\mathfrak{P}^{a([ie/n]+1)+b(n-i)}$

divides a_i $(i=1,2,\ldots,n-1)$. $\mathfrak{P}^{ae}$ divides a_n exactly by the

hypothesis.

Claim: ae = bn. Suppose bn>ae. Then for $(i=1,2,\ldots,n-1)$

$$a([ie/n]+1) + b(n-i) > a(ie/n) + (ae/n)(n-i) = ae$$

Since ζ is a root of f(x) we have

$$(1) \qquad \zeta^n + p^{e/n+1}b_1\zeta^{n-1} + \ldots + p^e b_n = 0$$

but $\mathfrak{P}^{ae}$ divides the last term of (1) exactly while a higher

power of $\mathfrak{P}$ divides the remaining terms which is a contradiction.

Thus $bn \leq ae$. Now suppose that $bn < ae$, then for $(i=1,2,\ldots,n-1)$

$$\begin{aligned} a([ie/n]+1)+b(n-i) &> a(ie/n)+b(n-i) \\ &> bn(i/n)+b(n-i) \\ &= bn \end{aligned}$$

and p^{bn} divides the first term of (1) exactly while a higher power of p divides the remaining terms. Again a contradiction. Hence bn = ae.

Since (e,n) = 1 we have that a = a'n and b = b'e

$\rightarrow$ a'ne = b'ne

$\rightarrow$ a' = b'

so we can write a = rn and b = rn where $r \in Z^+$. Since p is divisible by p^{rn} we have by Proposition I that $[Q[\zeta],Q] \geq rn$ but $[Q[\zeta],Q] \leq n$ $\rightarrow$ r=1 and $[Q[\zeta],Q] = n$. Thus f(x) is irreducible.

∎

2.4 PERRON'S GENERALIZATION

2.4.1 *Theorem* (Perron)

Let $p_1, p_2, \ldots, p_s$ be rational primes. Then the polynomial

$$f(x) = x^n + \prod_{k=1}^{s} p_k^{[e_k/n]+1} a_1 x^{n-1} + \prod_{k=1}^{s} p_k^{2e_k/n+1} a_2 x^{n-2} + \ldots + \prod_{k=1}^{s} p_k^{(n-1)e_k/n+1} a_{n-1} x + \prod_{k=1}^{s} p_k^{e_k} a_n$$

where:

(i) $a_i \in Z$ $(i=1,2,\ldots,n)$

(ii) $(a_n,p_k) = 1$ $(k=1,2,\ldots,s)$

(iii) $(n,e_1,e_2,\ldots,e_s) = 1$,

is irreducible.

Proof. Let $\mathbb{Q}[\zeta]$ be an extension of $\mathbb{Q}$ where $f(\zeta) = 0$. Then as in the previous theorems there is a nontrivial prime ideal factor P_j of ζ and p_j. Let a_j be the highest power of P_j that divides p_j and b_j the highest power of P_j that divides ζ. Then as in the previous theorem we have $a_j e_j = b_j n$. If we let $d_j = (n, e_j)$ then there is a natural number r_j such that $a_j = r_j(n/d_j)$ and $b_j = r_j(n/d_j)$. Therefore for $(j=1,2,\ldots,s)$ we have that

(1) $\qquad p_j$ is exactly divisible by $P_j^{r_j(n/d_j)}$

Now (1) holds for each prime ideal factor of p_j in $\mathbb{Q}[\zeta]$ hence

$$p_j = \prod P_{jk}^{r_{jk}\, n/d_j} = A^{n/d_j}.$$

where the product extends over all prime factors P_{jk} of p_j in $\mathbb{Q}[\zeta]$.

Therefore by Proposition *II* n/d_j divides $[\mathbb{Q}[\zeta], \mathbb{Q}]$ for $(j=1,2,\ldots,s)$. But by hypothesis $(d_1, d_2, \ldots, d_m) = 1$ hence $n \mid [\mathbb{Q}[\zeta], \mathbb{Q}] = n$ which implies that $[\mathbb{Q}[\zeta], \mathbb{Q}] = n$ and $f(x)$ is irreducible.

∎

III. NEWTON POLYGONS

3.1 INTRODUCTION

A polygon is associated with each polynomial f(x) for which a multiplication theorem holds. The polygon may yield irreducibility criteria. Before introducing Newton polygons we will introduce the p-adic representation of the rationals where p is an arbitrary rational prime.

3.2 REPRESENTATIONS IN THE DOMAIN OF P

3.2.1 *Definition* Let p be an arbitrary but fixed rational prime. If $u \in Z^+$ then u may be written

$$u = a_0 + a_1 p + \ldots + a_n p^n \tag{1}$$

The right-hand-side of (1) is called a *representation of u in the domain of p.*

The representation (1) is not unique for u may also be written $u = (a_0+p) + (a_1-1)p + \ldots + a_n p^n$.

3.2.2 *Definition* If in (1), $0 \leq a_i \leq p-1$ for $(i=1,2,\ldots,n)$ then (1) is called a *reduced representation of u in the domain of p.*

A representation, reduced or not, will sometimes be denoted

$$u = a_0, a_1 a_2 \ldots a_n \qquad (p)$$

3.2.3 *Proposition* The reduced representation of an integer $u \in Z^+$ is unique.

Proof. Suppose $u = a_0, a_1 \ldots a_m = b_0, b_1 \ldots b_n \quad (p)$

Both representations of u may be extended to a sequence by adjoining a countable number of zeros. Then $u \equiv a_0 \equiv b_0 \pmod{p}$ and since $0 \leq a_0 < p$ and $0 \leq b_0 < p$, $a_0 = b_0$. Now make the inductive assumption that $a_i = b_i$ for $i \leq n$. Then

$$u - \sum_{i=0}^{n} a_i p^i \equiv a_{n+1} \equiv b_{n+1} \pmod{p^{n+2}}$$

which implies $a_{n+1} = b_{n+1}$.

∎

3.2.4 *Definition* Generalizing (1) the class of representations with respect to a rational prime p is defined to be the set:

$$\{A = \sum_{i=m}^{\infty} a_i p^i \mid m \in Z,\ a_i \in Z\}$$

3.2.5 *Definition* If $m \geq 0$ in Definition 3.2.4, then

$$A = a_0, a_1 \ldots a_n \ldots \quad (p)$$

is said to be an *integer in the domain of p.*

Arithmetic operations may be performed on representations in a natural way. If

$$A = \sum_{i=m}^{\infty} a_i p^i$$

and

$$B = \sum_{i=n}^{\infty} b_i p^i$$

are two representations, then

$$A \pm B = \sum_{i=\min\{m,n\}}^{\infty} (a_i \pm b_i) p^i$$

and

$$AB = \sum_{i=m+n}^{\infty} \left(\sum_{j+k=i} a_j b_k \right) p^i$$

The quotient A/B is defined to be the representation C such that A = BC. The representation C can be found by solving the following sequence of congruences:

$$b_n b'_{-n} \equiv 1 \pmod{p^{n+1}}$$

$$(b_n + b_{n+1}p)(b'_{-n} + b'_{-n+1}p) \equiv 1 \pmod{p^{n+2}}$$

$$\vdots$$

(2)

$$(b_n + b_{n+1}p + \ldots + b_{n+k}p^k)(b'_{-n} + b'_{-n+1}p + \ldots + b'_{-n+k}p^k) \equiv 1 \pmod{p^{k+1}}$$

$$\vdots$$

The reduced representation of a rational number is always periodic [1] p.40. Thus the system of congruences (2) is finite if the b'_k's are choosen so that $0 \leq b'_k < p$ for $(k=-n,-n+1,\ldots)$ Setting $B' = \sum_{i=-n}^{\infty} b'_i p^i$ we obtain $BB' = 1$ and $C = AB'$. Note that the representations that result from these operations are not necessarily reduced even when A and B are.

In practice an arbitrary rational u/v may be written $u/v = \pm p^k (r/s)$ where $r,s \in Z$ and $(r,p)=(s,p)=(r,s)=1$.

The representation for r and s are easily found since they are integers. The representation for the quotient can then be obtained by long division. If $r/s = \sum_{i=0}^{\infty} a_i p^i$ then $|u/v| = p^k(r/s) = \sum_{i=0}^{\infty} a_i p^{i+k}$. If $u/v<0$ then since

$$0 = p^k+(p-1)p^{k+1}+(p-1)p^{k+2}+ \ldots$$

$$u/v = 0-|u/v| = \left(\sum_{i=1}^{\infty} (p-1-a_i)p^{i+k} \right) + (1-a_0)p^k$$

The following examples illustrate calculations with representations.

3.2.6 *Examples* Let p=7, then

(i)

$$\begin{array}{rcl} 2301 & = & 5,646\overline{0} \\ +4917 & = & 3,22020 \\ \hline 7218 & = & 1,20030 \end{array}$$

(ii)

$$\begin{array}{rcl} 0 & = & 7,6666\overline{6} \\ -4917 & = & -3,22020 \\ \hline -4917 & & 4,4464\overline{6} \end{array}$$

(iii)

$$\begin{array}{rcl} 2145 & = & 3,5160\overline{0} \\ -7062 & = & -6,0462\overline{0} \\ \hline -4917 & & 4,4464\overline{6} \end{array}$$

(iv)

$$\begin{array}{rcl} 418 & = & 5,311\overline{0} \\ \times 117 & = & \times 5,220\overline{0} \\ \hline 48906 & & 4,406 \\ & & \quad 3032 \\ & & \quad\quad 3032 \\ \hline & & 4,0426\overline{0} \end{array}$$

(v) For this example let p=5. To find the representation of 7/31 in the domain of 5 first find the representation of $7 = 2,1\overline{0}$ and $5 = 1,11\overline{0}$. then

$$
\begin{array}{l}
2,1 = 2,15\overline{4} \\
\quad\underline{2,22} \\
\quad\quad 424\overline{4} \\
\quad\quad\underline{444} \\
\quad\quad\quad 343\overline{4} \\
\quad\quad\quad\underline{333} \\
\quad\quad\quad\quad 104\overline{4} \\
\quad\quad\quad\quad\underline{111} \\
\quad\quad\quad\quad\quad 424\overline{4}
\end{array}
\qquad
\begin{array}{l}
1,11 \\
\hline
2,431\overline{431}
\end{array}
$$

thus $7/31 = 2,\overline{431}$ in the domain of p=5.

3.3 HENSEL'S LEMMA

3.3.1 *Definition* Let P(x) be a polynomial of the form:

(1) $$P(x) = A_0x^n + A_1x^{n-1} + \ldots + A_n \qquad (p)$$

where $$A_i = a_{\rho_i}p^{\rho_i} + a_{\rho_i+1}p^{\rho_i+1} + \ldots$$

for (i=1,2,...,n). Then P(x) is said to be *a polynomial in the domain of p.*

Hensel has shown [7] p.78 how, in a finite number of steps, to determine if a polynomial in the domain of p is reducible or not. A special application of this result is the following theorem., [7] section 4.

3.3.2 *Theorem* (*Hensel's Lemma*)

Let $P(x) = x^n + A_1x^{n-1} + \ldots + A_n \quad (p)$

be a monic polynomial in the domain of p whose coefficients A_i are integers in the domain of p. If there exists two polynomials f(x) and g(x) with rational integral coefficients such that $(f(x),g(x)) \not\equiv 0 \pmod{p}$ and $P(x) = f(x)g(x) \pmod{p}$ then P(x) is reducible in the domain of p.

3.4 REPRESENTATIONS IN THE DOMAIN OF $p^{1/s}$

Shortly we will be interested in representations with respect to powers of $p^{1/s}$ where p is a rational prime and s is a positive integer. A polynomial in the domain of $p^{1/s}$ will have the form of Definition 3.3.1 with the exception that the coefficients' representations are in powers of $p^{1/s}$ instead of powers of p.

3.4.1 *Lemma* If $A = a_0 + a_1p^{1/s} + a_2p^{2/s} + \ldots$ where $0 \leq a_i < p \quad (i=0,1,2,\ldots)$ then there exists a $B = b_0 + b_1p^{1/s} + \ldots$ where $0 \leq b_i < p \quad (i=0,1,2,\ldots)$ such that

$$AB = 1 \qquad (p^{1/s})$$

Furthermore if A and $B \not\equiv 0$ are two representations in the domain of $p^{1/s}$, then there exists a representation C in the domain of $p^{1/s}$ such that A=BC.

Proof. Suppose $a_0 \not\equiv 0$. Then the following system of congruences may be solved for $b_0, b_1, \ldots$

$$a_0b_0 \equiv 1 \pmod{p^{1/s}}$$

$$(a_0+a_1p^{1/s})(b_0+b_1p^{1/s}) \equiv 1 \pmod{p^{2/s}}$$

.

.

.

$$\left(\sum_{i=0}^{k} a_i p^{i/s}\right)\left(\sum_{i=0}^{k} b_i p^{i/s}\right) \equiv 1 \pmod{p^{(k+1)/s}}$$

.

.

.

If $a_0=0$ then $A = a_o p^{\rho/s} + a_1 p^{(\rho+1)/s} + \ldots$

where a_0 is the first nonzero integer in the representation of A and ρ is a positive integer. Then

$$A = p^{\rho/s}(a_0 + a_1 p^{1/s} + \ldots)$$

$$= p^{\rho/s} A'$$

By the above there exists a B' such that

$$A'B' = 1 \qquad (p^{1/s})$$

Set $B = p^{-\rho/s}B'$ and thus $AB = p^{\rho/s}A'p^{-\rho/s}B' = A'B' = 1 \quad (p^{1/s})$

Now if A and $B \neq 0$ are two representations in the domain of $p^{1/s}$ then there exists a B' in the domain of $p^{1/s}$ such that

$$BB' = 1 \qquad (p^{1/s})$$

thus $$C = AB' \qquad (p^{1/s})$$

■

3.4.2 *Theorem* If

$$P(x) = A_0x^m + A_1x^{m-1} + \ldots A_m \qquad (p^{1/s})$$

and

$$Q(x) = B_0x^n + B_1x^{n-1} + \ldots B_n \qquad (p^{1/s})$$

where the degP=m≥n=degQ and the coefficients of P(x) and Q(x) are integers in the domain of $p^{1/s}$, then the greatest common divisor of P and Q, (P,Q) exists in the domain of $p^{1/s}$.

Proof. By Lemma 3.4.1 and the hypothesis, $A_0 \neq 0 \neq B_0$, hence there exists a C_0 in the domain of $p^{1/s}$ such that $A_0=B_0C_0$.

Then

$$P(x)-C_0x^{m-n}Q(x) = R(x) \qquad (p^{1/s})$$

is a polynomial of degree strictly less than n.

Since this is the key step in the Euclidean Algorithm, the gcd exists in the domain of $p^{1/s}$.

∎

3.4.3 *Corollary* Theorem 3.4.1 holds in the domain of p.

Proof. Set s=1.

3.5 THE NEWTON POLYGON OF A POLYNOMIAL

3.5.1 *Definition* Let $P(x)=a_0x^n + \ldots + a_n$ be a polynomial with rational coefficients. Then for $a_i \neq 0$, a_i can be written $a_i=p^{\alpha}(r_i/s_i) = p^{\alpha}A_i$ where A_i is the representation of r_i/s_i with respect to p. Since $(p,r_i)=(p,s_i)=(r_i,s_i)=1$, A_i is an integer with respect to p. Thus every polynomial $P(x)\varepsilon Q[x]$ can be written

$$P(x) = \sum A_{\alpha\beta}p^{\alpha}x^{\beta}. \qquad (p)$$

P(x) is then *in the domain of p.*

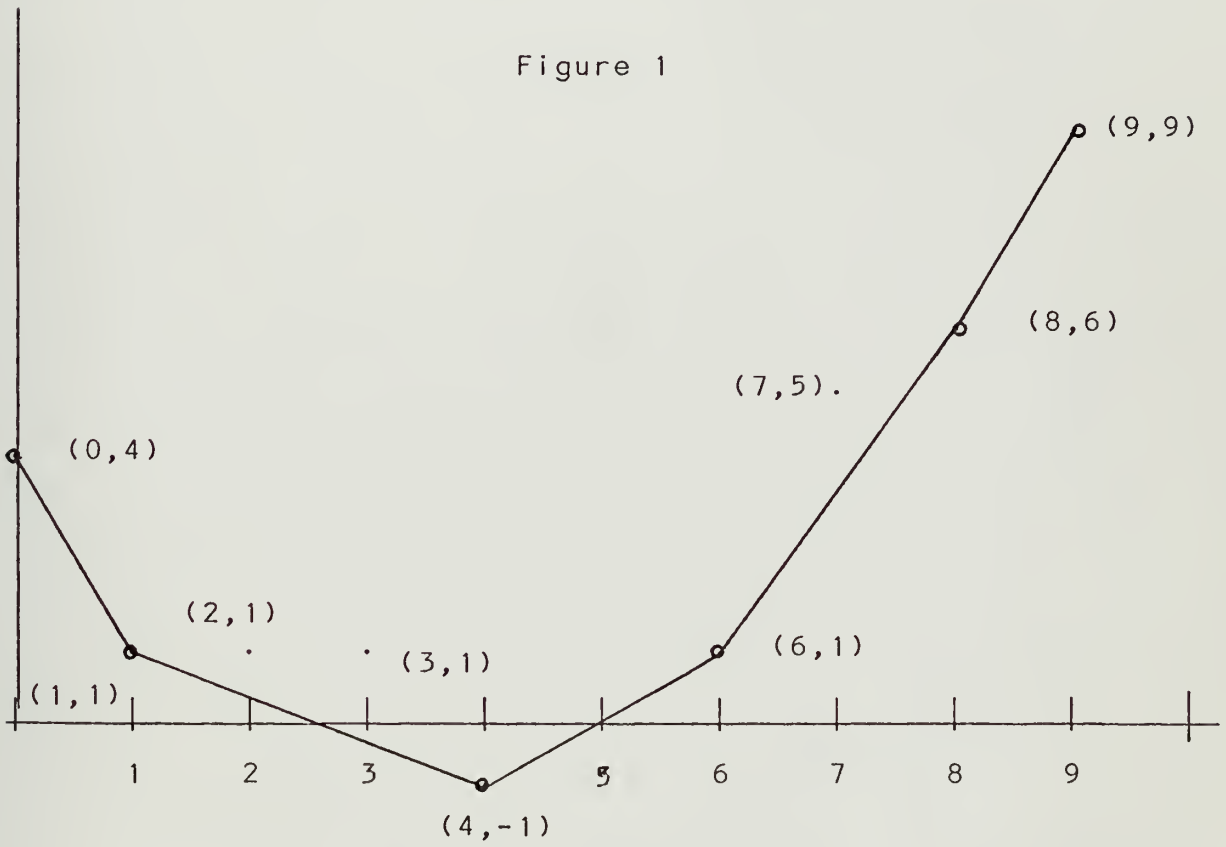
3.5.2 *Definition* The *Newton Polygon* of a polynomial in the domain of p, $P(x) = \sum A_{\alpha\beta} p^{\alpha} x^{\beta}$ is the lower convex hull of the ordered pairs (β,α), where $A_{\alpha\beta} \neq 0$, ordered according to the β's. The ordered pair (β,α) is called the *representative point* of the term $A_{\alpha\beta}$.

3.5.3 *Example*

Let $P(x) = 2^9x^9+5^{-2}2^6x^8+2^5x^7+2x^6+5^{\frac{1}{2}}-1x^4+2x^3+2x^4+2x+2^4$

Then Figure 1 is the Newton polygon of P(x) for p=2.

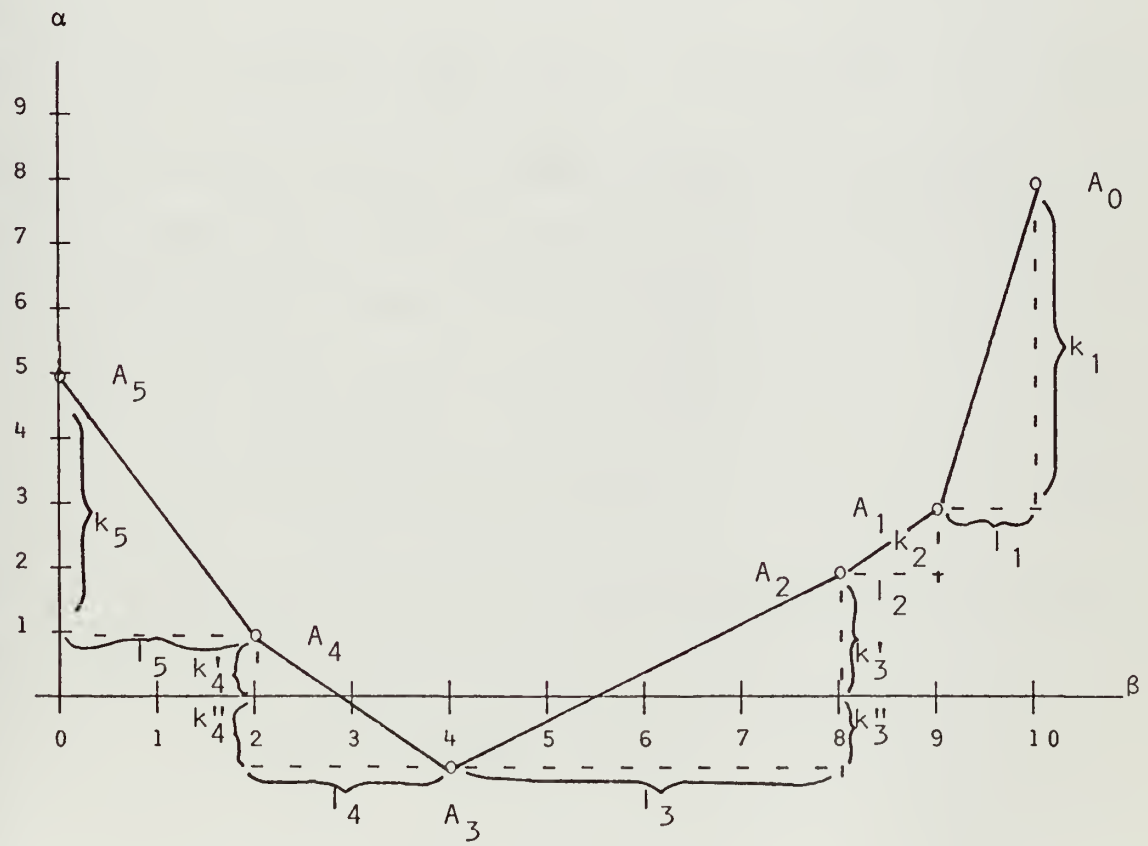
Figure 1



Let Figure 2 be the polygon of a polynomial $P(x)$. Label the vertices from right to left $A_0, A_1, \ldots, A_5$ and denote the i^{th} side by $A_{i-1}A_i$. By assigning the direction from right to left positive, the slope m_i of the i^{th} side $A_{i-1}A_i$ is determined. For example in Figure 2 the sides A_1A_2 and A_3A_4 have slopes $m_2 = -k_2/l_2$ and $m_4 = +k_4/l_4$ respectively.

By construction k_i and l_i are positive rational integers. Let $\lambda_i = (k_i, l_i)$. Then $k_i = \lambda_i r_i$ and $l_i = \lambda_i s_i$ where $(r_i, s_i) = 1$. Thus $m_i = r_i/s_i$. If $k_i = 0$ then set $\lambda_i = l_i$ and $s_i = 1$.

Figure 2



Let $k_4 = k'_4 + k''_4$ and $k_3 = k'_3 + k''_3$.

3.5.4 *Theorem*

Let

$$P(x) = \sum A_{\alpha\beta} p^{\alpha} x^{\beta} \qquad (p)$$

and

$$Q(x) = \sum B_{\alpha\beta} p^{\alpha} x^{\beta} \qquad (p)$$

be two polynomials in the domain of p of degrees m and n respectively. Then the polygon of the product of P(x) and Q(x) is obtained by adjoining the sides of the polygons of P(x) and Q(x) in the order of increasing slopes starting from the point $\Omega=(m+n, \rho+\tau)$ where ρ and τ are the exponents of p in the coefficients of x^m in P(x) and x^n in Q(x) respectively.

Proof. Let $P(x)Q(x) = \sum_{i=0}^{m+n} c_i x^{m+n-i} = \sum C_{\alpha\beta} p^{\alpha} x^{\beta}$. (p)

Then it is clear that the point Ω belongs to the Newton polygon of PQ since the representation of the coefficient c_0 of x^{m+n} in the product has the form

$$c_0 = a_0 b_0 = (A_{\rho m} p^{\rho})(B_{\tau n} p^{\tau}) \qquad (p)$$

$$= A_{\rho m} B_{\tau n} p^{\rho+\tau} . \qquad (p)$$

Now for an arbitrary rational 'a' define the function $V_p(a)=\alpha$ where $a=p^{\alpha}(r/s)$, $(r,p)=(s,p)=(r,s)=1$. Then

$$V_p(c_i) = V_p\left(\sum_{j+k=i} a_j b_k \right)$$

$$\geq \operatorname{Min}_{j+k=i} \{V_p(a_j b_k)\}$$

$$= V_p(a_j' b_k')$$

$$= V_p(a_j') + V_p(b_k') = \rho' + \tau'$$

Thus the ordered pair corresponding to $c_i x^{m+n-i}$ lies above $(m+n-j'-k', \rho'+\tau') = (m-j', \rho') + (n-k', \tau')$. But since $(m-j', \rho')$ lies on or above the polygon of $P(x)$ and $(n-k', \tau')$ lies on or above the polygon of $Q(x)$, the representative point corresponding to $c_i x^{m+n-i}$ lies on or above the polygon obtained in the theorem.

It remains to show that if $(m-j', \rho')$ and $(n-k', \tau')$ lie on the polygons of P and Q respectively, then $(m+n-i, V_p(c_i))$ lies on the polygon of the theorem. But if this is so then

$$V_p(a_j b_k) > V_p(a_{j'} b_{k'}) \quad j=j' \quad k=k'$$

which implies $$V_p(c_i) = V_p(a_{j'} b_{k'})$$

by Lemma 4.3.2, thus $(m+n-i, V_p(c_i))$ lies on the polygon of the theorem.

3.6 A REPRESENTATION OF A POLYNOMIAL P(x)

In this section we wish to establish a representation of a polynomial P(x) obtained from its polygon.

Suppose first that the polygon of P(x) is not a straight line. Let

$$P(x) = A_0 p^{\rho} x^n + A_1 x^{n-1} + \ldots + A_n \qquad (p)$$

where $A_0 = u/v$ is a non-zero rational such that $(u,p)=(v,p)=(u,v)=1$. Define $Q(x) = (1/A_0)P(x)$. Then P and Q have the same polygon. Without loss of generality Figure 2 can be assumed to be the polygon of Q(x). Then

$$n = l_1 + l_2 + \ldots + l_5$$

and $\rho = k_1+k_2+k_3'$.

The general form of the terms of $Q(x)$ whose representative points lie on the sides of the polygon are:

On A_0A_1,

$$f_1'(x) = x^{(l_5+l_4+l_3+l_2)}\left[a_1x^{(l_1)}p^{(k_1)}+\ldots+b_1x^{(\lambda_1-j)s_{1p}(\lambda_1-j)r_1}+\ldots+c_1\right]p^{(k_3'+k_2)} \quad ;$$

on A_1A_2,

$$f_2'(x) = x^{(l_5+l_4+l_3)}\left[a_2x^{(l_2)}p^{(k_2)}+\ldots+b_2x^{(\lambda_2-j)s_{2p}(\lambda_2-j)r_2}+\ldots+c_2\right]p^{k_2'};$$

on A_2A_3,

$$f_3'(x) = x^{(l_5+l_4)}\left[a_2x^{l_3}p^{k_3}+\ldots+b_3x^{(\lambda_3-j)s_{3p}(\lambda_3-j)r_3}+\ldots+c_3\right]p^{-k_3''} \quad ;$$

on A_3A_4,

$$f_4'(x) = x^{l_5}\left[a_4x^{l_4}+\ldots+b_4x^{(\lambda_4-j)s_{4p}jr_4}+\ldots+c_4p^{k_4}\right]p^{-k_4''} \quad ;$$

on A_4A_5,

$$f_5'(x) = \left[a_5x^{l_5}+\ldots+b_5x^{(\lambda_5-j)s_{5p}jr_5}+\ldots c_5p^{k_5}\right]p^{k_4'} \quad ,$$

where $a_i,b_i,c_i\varepsilon\{1,2,\ldots,p-1\}$, $a_i\neq 0\neq c_i$ for $(i=1,2,\ldots,5)$.

For each a_i in the previous expressions, there exists $a_i'\varepsilon\{1,2,\ldots,p-1\}$ such that $a_ia_i'\equiv 1 \pmod p$. Define $f_i(x)=a_i'f_i'(x)$ for $(i=1,2,\ldots,5)$ and denote the new coefficients of $f_i(x)$,$\{\ldots, b_i', \ldots, c_i'\}$ the smallest positive remainder modulo p obtained from the products $\{\ldots, a_i'b_i, \ldots, a_i'c_i, \ldots\}$.

If we let $k''=k_3''=k_4''$ then by Theorem 3.5.4 the polynomials $A_0 p^{k''} \prod f_i(x)$ and $P(x)$ have the same polygons. Thus we can write

$$(1) \qquad P(x) = A_0 p^{k''} \prod f_i(x) + \sum A_{\alpha\beta} p^{\alpha} x^{\beta} \qquad (p)$$

where the $\sum$ sign extends to those terms whose representative points lie above the polygon. By construction $\beta<n$.

Now suppose that the polygon of $P(x)$ is a straight line. Then by the same argument that led to (1) we can write

$$(2) \qquad P(x) = A_0 p^{k''} f(x) + \sum A_{\alpha\beta} p^{\alpha} x^{\beta} \qquad (p)$$

where $f(x)$ has one of the following two forms:

$$x^{l} p^{k} + \ldots + b x^{(\lambda-j)s} p^{(\lambda-j)r} + \ldots + c$$

or

$$x^{l} + \ldots + b x^{(\lambda-j)s} p^{jr} + \ldots + c$$

as the polygon of $P(x)$ has negative or positive slope respectively.

Suppose $f(x)$ has the second form. Then we can make the substitution

$$x^{s} = y p^{r} .$$

Dividing the result by p^{k} we obtain a polynomial

$$g(y) = y + \ldots b y^{(\lambda-j)} + \ldots + c$$

Suppose $\qquad g(y) \equiv \prod (g_i(y))^{m_i} \pmod{p}$

where $g_i(y) = y^{n_i} + \ldots + b_i y^{(n_i-j)} + \ldots + c_i$

Then we can write

$$g(y) + \prod (g_i(y))^{m_i} + p\Phi(y)$$

where $\Phi(y)$ is of degree $<\lambda$.

Then

$$f(x) = p^k(\prod (g_i(x^s/p^r))^{m_i} + p\Phi(x^s/p^r))$$

Set $G_i(x) = p^{n_i r} g_i(x^s/p^r)$

then we obtain

$$f(x) = \prod (G_i(x))^{m_i} + p^{k+1}\Phi(x^s/p^r)$$

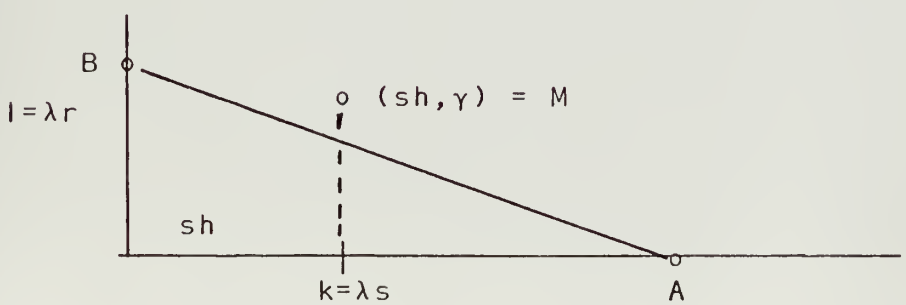
since $n_i m_i = \lambda$.

An arbitrary term of $p^{k+1}\Phi(x^s/p^r)$ has the form

$$p^{k+1} a(x^s/p^r)^h$$

where $h<\lambda$ and a is an integer divisible by p. If Figure 3 is the polygon of f(x), then the representative point of the

Figure 3



term has coordinates (sh,γ) where $\gamma \geq k+1-rh$. The point M lies above the polygon AB since

$$\frac{k+1-rh}{(\lambda-h)s} = \frac{(\lambda-h)r+1}{(\lambda-h)s}$$

$$= \frac{r}{s} + \frac{1}{(\lambda-h)s} > \frac{r}{s} \quad .$$

The polynomials $G_i(x)$ have integer coefficients and their polygons are straight lines with the same slope as AB. We can then write (2) as

$$P(x) = A_0 p^{k''} \prod (G_i(x))^{M_i} + \sum A_{\alpha\beta} p^{\alpha} x^{\beta}$$

By applying this result to the polynomials $f_i(x)$ of (1) corresponding to the sides of the polygon of P(x) and denoting the polynomials by $f_{ij}(x)$, we obtain the following representation of P(x):

$$(3) \qquad P(x) = A_0 p^{k''} \prod (f_{ij}(x))^{m_i} + \sum A_{\alpha\beta} p^{\alpha} x^{\beta} \quad .$$

3.7 THE FUNDAMENTAL THEOREM

3.7.1 *Theorem* Every polynomial P(x) whose coefficients can be expressed as a representation in p and whose polygon is not a straight line, is reducible in the domain of p. Furthermore to an arbitrary side $A_{i-1}A_i$ corresponds a divisor of P(x) in the domain of p whose polygon is a straight line of the same length and slope as the side $A_{i-1}A_i$.

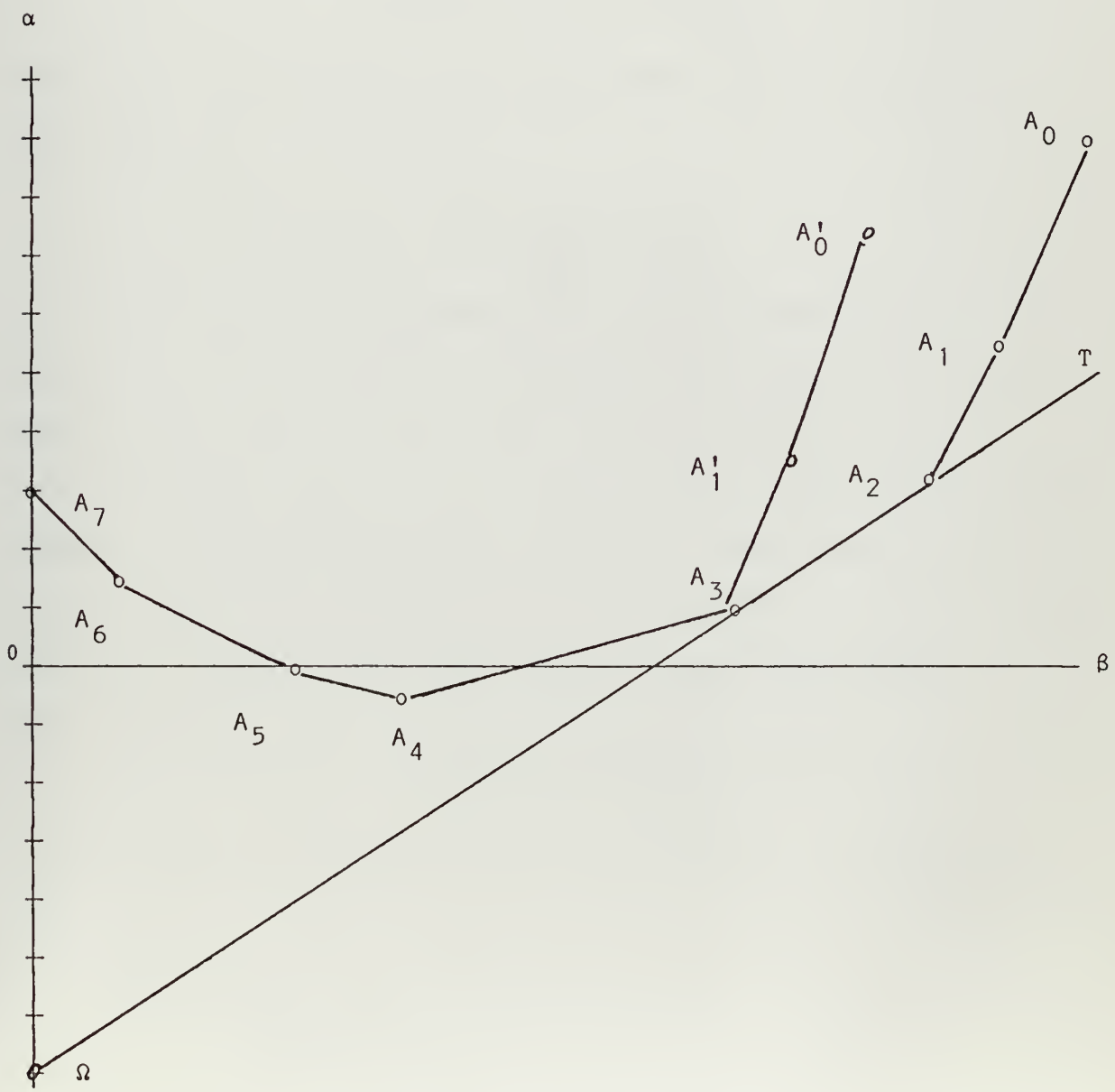
Proof. Let $P(x) = A_0 p^{\rho} x^n + A_1 x^{n-1} + \ldots + A_n$, $A_0 \neq 0$ and set $Q(x) = (1/A_0)P(x)$. Since P and Q have the same

polygon, the theorem will hold for P if it holds for Q. From section 3.6 (1) Q(x) may be written

$$(1) \qquad Q(x) = p^{k''}\prod f_i(x) + \sum A_{\alpha\beta} p^{\alpha} x^{\beta}.$$

We can suppose without loss of generality that Figure 4 represents the polygon of Q(x). The theorem will be established for the side A_2A_3. Let $\lambda=(k_3,l_3)$, $r=k_3/\lambda$ and $s=l_3/\lambda$.

Figure 4



Then $m=-r/s$ since the slope of A_2A_3 is negative. A point of Figure 4 whose coordinates are rational integers will be called a *grid point*. Consider the family of all straight lines passing through a grid point with slope m. There will then be a vertical separation of 1/s between any two adjacent lines. If $N=(\beta,\alpha)$ and $N'=(\beta',\alpha')$ are any two grid points, then the vertical separation between the lines of this family passing through N and N' is

$$|(\alpha'-\alpha) + (\beta'-\beta)(r/s)|$$

Note that since $(r,s)=1$, we can always find α, α', β, β' such that

$$(\alpha'-\alpha) + (\beta'-\beta)(r/s)=1/s.$$

By extending the side A_2A_3 we obtain the line ΩT. If $N=(\beta,\alpha)$ is an arbitrary grid point, let n denote the intersection of a line through N and parallel to ΩT with the ordinate axis. The ordinate axis and the line ΩT then become a new coordinate system which, with an appropriate change of scale, yield the coordinates of $N=(|nN|,|\Omega n|)$. By the change of scale $|nN|=\beta$. Also there exists a positive integer η such that

$$|\Omega n|=\eta/s$$

η will always be positive since the polygon lies above the ΩT axis.

From Figure 4 we also have

$$|On|-|O\Omega|=|\Omega n|$$

that is

$$(2) \qquad (\alpha - \beta r/s) - \{k' - (l_4 + l_5 + \ldots + l_8)(r/s)\} = \eta/s$$

In the representation (1) of $Q(x)$ make the change of variables

$$(3) \qquad x = yp^{-r/s} = yp^{m}$$

and define

$$Q(y, p^{1/s}) = p^{-\{k' - (l_4 + l_5 + \ldots + l_8)(r/s)\}} Q(yp^{m}) .$$

Then to each term of $Q(x)$ of the form $A \; p \; x$ we obtain a corresponding term of $Q(y, p^{1/s})$ of the form

$$A_{\alpha\beta} p^{\alpha - \{k' - (l_4 + l_5 + \ldots + l_8)(r/s)\} - \beta r/s} y$$

which because of (2) reduces to

$$A_{\alpha\beta} p^{\eta/s} y^{\beta} .$$

Therefore the polygon of $A_0 A_1 \ldots A_7$ can be considered the polygon of $Q(y, p^{1/s})$ in the domain of $p^{1/s}$ and from (1) and (3) $Q(y, p^{1/s})$ can be written

$$(4) \qquad Q(y, p^{1/s}) = g_i(y, p^{1/s}) + \sum A_{\alpha\beta} p^{\eta/s} y^{\beta} .$$

where $g_i(y, p^{1/s})$ is equal to $f_i(yp^{m})$ up to a factor which is an integer power of $p^{1/s}$.

From Figure 4 the form of $g_i(y, p^{1/s})$ can be obtained. For example:

$$g_6(y, p^{1/s}) = y^{\lambda_6 s_6 + \ldots + b_6 p^{j\tau/s} y^{(\lambda_6 - j)s_6 + \ldots + c_6 p^{\lambda_6 \tau/s}}} ;$$

$$g_2(y,p^{1/s}) = p^{\lambda_2'\tau/s)}y^{\lambda_2 s}{}_2+\ldots+b_2p^{(\lambda_2-j)\tau/s}y^{(\lambda_2-j)s}{}_2+\ldots+c_2;$$

$$g_3(y,p^{1/s}) = g(y) = y^{\lambda s}+\ldots+by^{(\lambda-1)s}+\ldots+c$$

where $\tau\varepsilon Z^+$ and $b_i,d_i\varepsilon\{0,1,\ldots,p-1\}$, $c_i\not\equiv 0$.

Since g_3 is monic, $(g_i,g_3)\not\equiv 0 \pmod p$ for $i\not\equiv 3$. (g_i,g_3) is a polynomial in y with integral coefficients in the domain of $p^{1/s}$. Now define

$$G(y) = \prod_{i\not\equiv 3} g_i(y,p^{1/s})$$

and $$H(y) = g_3(y,p^{1/s}) \quad .$$

Claim: $Q(y,p^{1/s})$ can be decomposed into the product of two factors in the domain of $p^{1/s}$

$$Q(y,p^{1/s}) = G'(y)H'(y) \qquad (p^{1/s}) \tag{5}$$

where

$$G'(y) = G(y) + \sum A_{\alpha\beta}p^{\alpha/s}y^{\beta}$$

and $$H'(y) = H(y) + \sum A_{\alpha\beta}p^{\alpha/s}y^{\beta}$$

$\alpha\varepsilon Z^+$.

From (4)

$$Q(y,p^{1/s}) \equiv G(y)H(y) \pmod{p^{1/s}}$$

To establish the decomposition of $Q(y,p^{1/s})$ it need only be shown that for $\alpha\geq 1$, the congruence

$$Q(y,p^{1/s}) \equiv G'H' \pmod{p^{\alpha/s}} \tag{6}$$

where $G' = G + p^{1/s}G_1 + \ldots + p^{(\alpha-1)/s}G_{\alpha-1}$

and $H' = H + p^{1/s}H_1 + \ldots + p^{(\alpha-1)/s}H_{\alpha-1}$

implies the congruence

$$(7) \qquad Q(y,p^{1/s}) \equiv (G' + p^{\alpha/s}G_\alpha)(H' + p^{\alpha/s}H_\alpha) \pmod{p^{(\alpha+1)/s}}.$$

From (6) there exists a polynomial $L(y)$ with integer coefficients and of degree less than the degree of Q such that

$$Q(y,p^{1/s}) - G'H' \quad p^{\alpha/s}L(y) \pmod{p^{(\alpha+1)/s}}.$$

Hence (7) follows provided there exist polynomials G and H such that

$$L \equiv H'G_\alpha + G'H_\alpha \pmod{p^{1/s}}.$$

But this follows since $p^{1/s} \mid (G',H')$. Thus there exist G'_α and H'_α such that

$$H'G'_\alpha + G'H'_\alpha \equiv (G',H') \pmod{p^{1/s}}$$

which in turn implies

$$H'\left(\frac{G'_\alpha}{(G',H')}\right) + G'\left(\frac{H'_\alpha}{(G',H')}\right) \equiv 1 \pmod{p^{1/s}}.$$

Hence $$L \equiv H'\left(\frac{LG'_\alpha}{(G',H')}\right) + G'\left(\frac{LH'_\alpha}{(G',H')}\right) \text{(Mod } p^{1/s})$$

and (5) is established.

Now in $p^{\{k'+(1+\ldots+1)(r/s)\}}G'(y)$ and $H'(y)$ make the change of variables

$$y = xp^{r/s}$$

and denote the new polynomials $G(x)$ and $H(x)$. Note these polynomials have coefficients in the domain of $p^{1/s}$ of the form $A_{\alpha\beta}p^{\alpha/s}x^{\beta}$.

The polygons of G and H can be plotted in the usual way by assigning the representative points $(\beta,\alpha/s)$ to the above term. Plotting G using the axis $\beta 0\alpha$ in Figure 4 we obtain the polygon $A_0'A_1A_2 \ldots A_7$, and for H a polygon of one side with the same slope and length as A_2A_3. By the claim just established, G and H have no common divisors in the domain of $p^{1/s}$.

Now make the change of variables $x = y\omega^{-r}p^{m}$ instead of $x = yp^{m}$, where ω is the s^{th} root of unity. Then

$$Q(x) = H(x,\omega p^{1/s})G(x,\omega p^{1/s}) \qquad (p^{1/s})$$

vice $\quad Q(x) = H(x,p^{1/s})G(x,p^{1/s})$,

since $\quad (H(x,\omega p^{1/s}),\ G(x,\omega p^{1/s}))=1$

and $\quad (H(x,p^{1/s}),G(x,p^{1/s}))=1.$

Hence $\quad H(x,p^{1/s}) = H(x,\omega p^{1/s})$

and $\quad G(x,p^{1/s}) = G(x,\omega p^{1/s}).$

but since $H(x,p^{1/s}) \equiv H(x)$ and $G(x,p^{1/s}) \equiv G(x)$, their coefficients do not depend on $p^{1/s}$ but only on p, hence

$$Q(x) = H(x)G(x) . \qquad (p)$$

Extending this result to the remaining sides of the polygon yields

$$P(x) = P_1(x)P_2(x). \ . \ .P_7(x) \qquad (p)$$

where $P_i(x)$ corresponds to the i^{th} side of the polygon of $P(x)$.

■

3.8 APPLICATIONS

Let $f(x) = a_0x^n + \ . \ . \ . + a_n$ be a polynomial with rational coefficients and let $F(x) = A_0x^n + \ . \ . \ . + A_n$ be the corresponding polynomial with coefficients in the domain of p. Each factor $f_i(x)$ of $f(x)$ in $Q[x]$ has a corresponding factor $F_i(x)$ of $F(x)$ in the domain of p. If $G(x)|F(x)$ in the domain of p then the degree of $G = d = \sum \mu_i s_i$ where $0 \leq \mu_i \leq \lambda_i$. Since the degree of any factor $f_i(x)$ is equal to the degree of $G(x)$ for some divisor of $F(x)$ in the domain of p, we have the following propositions.

3.8.1 *Proposition* If $f_i(x)$ is a factor of $f(x)$ then the $\deg f_i = \sum \mu_i s_i$ where $0 \leq \mu_i \leq \lambda_i$.

3.8.2 *1^{st} Irreducibility Criterion* If the polygon of $f(x)$ is a straight line of slope $n=k/l=\lambda r/\lambda s=r/s$ then the degree of any divisor of $f(x)$ must be equal to $s, 2s, \ . \ . \ ., (\lambda-1)s$. In particular if $(k,l)=1$ then $f(x)$ is irreducible.

3.8.3 *2nd Irreducibility Criterion* If $f(x) \in Q[x]$ and $p^1, p^2, \ldots, p^k$ are k rational primes and

$$\sum \mu_i^1 s_i^1, \quad \sum \mu_i^2 s_i^2, \ldots, \quad \sum \mu_i^k s_i^k$$

represent the respective degrees of a divisor of $f(x)$ $F^i(x)$ in the domain of p^i, then the degree of an irreducible factor of $f(x)$ must simultaneously be representable as $\sum \mu_i^j s_i^j$ $(j=1,2,\ldots,k)$.

3.8.4 *Example* Let $f(x) = 25x^8 - 3x^3 + 15x^2 + 45$, then for $p=5$ the polygon of $f(x)$ is shown in Figure 5.

Figure 5

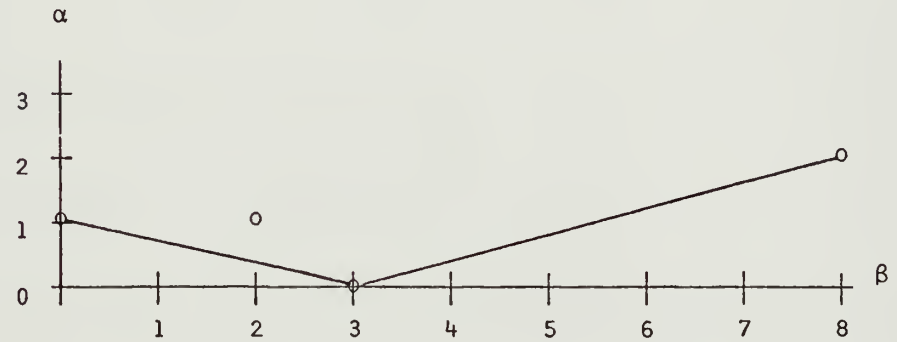


Figure 5 yields the following values:

$k_1 = 2 = r_1$ $\qquad$ $k_2 = 1 = r_2$

$l_1 = 5 = s_1$ $\qquad$ $l_2 = 3 = s_2$

$\lambda_1 = 1$ $\qquad$ $\lambda_2 = 1$

Hence $\sum \mu_i s_i = 3$ or 5.

If, on the other hand, $p=3$, then Figure 6 is the polygon of $f(x)$.

Figure 6

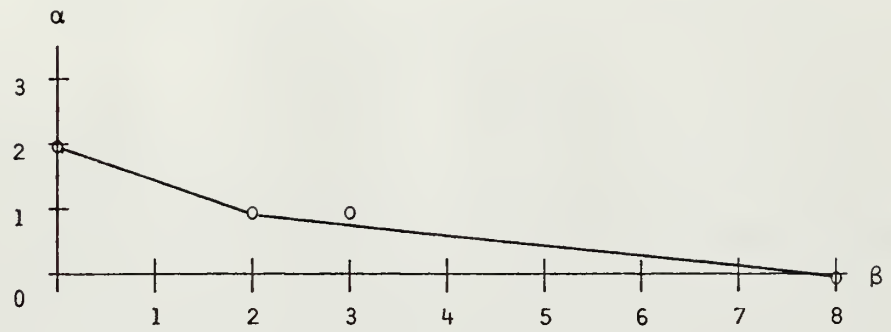


Figure 6 yields the following values:

$k_1=1=r_1$ $\qquad$ $k_2=1=r_2$

$l_1=6=s_1$ $\qquad$ $l_2=2=s_2$

$\lambda_1=1$ $\qquad$ $\lambda_2=1$

Hence $\sum \mu_i s_i = 2$ or 6.

Thus f(x) is irreducible.

Grace Murray Hopper[1] has extended the work of Dumas by associating with a polynomial a closed convex polygon for which an appropriate multiplication theorem holds.

[1]Hopper, Grace Murray, *New Types of Irreducibility Criteria*, Ph.D. Dissertation, Yale University, 1934.

IV. NON-ARCHIMEDEAN VALUES AND IRREDUCIBILITY OVER THE RATIONALS

4.1 INTRODUCTION

This section introduces the notion of a non-Archimedean absolute value on the ring $Q[x]$. The characterization of these values yields theorems on irreducibility which contain and extend the previous criteria.

4.2 ABSOLUTE VALUES

4.2.1 *Definition* A *non-Archimedean value* V on a ring R is a mapping from R into the extended reals R such that for all $a,b \in R$, the following properties hold:

(i) Va is unique

(ii) *(Triangle Law)* $V(a+b) \geq \min\{Va, Vb\}$

(iii) *(Product Law)* $V(ab) = Va + Vb$

(iv) $V(0) = \infty$ where 0 is the additive identity of R.

4.2.2 *Example 1* Let $V(a)=0$ for all $a \neq 0$ in R and $V(0)=\infty$. This is the *trivial* value on R. Henceforth only non-trivial non-Archimedean absolute values will be considered and will be refered to simply as *values*.

4.2.3 *Example 2* If the ring R is taken to be the rationals, then for an arbitrary but fixed prime p, each non-zero rational $a/b = p^k(u/v)$ where $(u,v)=(u,p)=(v,p)=1$. Define the map V_p as follows:

$$V_p(a/b)=k \qquad \text{for } a/b\neq 0$$

$$\text{and } V_p(0)=\infty$$

V_p is called the *p-adic value on* $\mathbb{Q}$.

4.2.4 *Definition* Two values V and V' on R are said to be *equivalent* if there is a positive real number c such that

$$V(a)=cV'(a) \text{ for all } a\in R.$$

McCarthy [15] p. 75-77 shows that every non-trivial non-Archimedean value on $\mathbb{Q}$ is equivalent to a p-adic value on $\mathbb{Q}$.

4.3 PROPERTIES OF VALUES

4.3.1 *Lemma* Let V be a value on a ring R and let R have a multiplicative identity 1, then:

(i) $V(1)=0$

(ii) $V(-1)=0$

(iii) $V(-a)=V(a)$ for $a\neq 0$

(iv) If a is an unit in R then $V(1/a)=-V(a)$

(v) for n , $V(a^n)=nV(a)$

Proof. $V(1)=V(1^2)=V(1)+V(1)$ implies $V(1)=0$ which establishes *(i)*, *(ii)* follows in a like manner and *(iii)* follows from *(ii)* by use of the product law. *(iv)* holds since

$$0=V(1)=V(a/a)=V(a)+V(1/a).$$

(v) follows by induction on n and *(iii)*.

Note: by *(v)* it needed not have been assumed that $V(0)=\infty$ since $V(0)=V(a^n-a^n)\geq\min\{V(a^n),V(a^n)\}=nV(a)$, thus $V(0)\geq nV(a)$ for all a in R and integers n which implies $V(0)=\infty$.

■

4.3.2 *Lemma* *(Strong Triangle Law)* If $V(a)=V(b)$ then

$$V(a+b)=\min Va,Vb$$

Proof. Suppose not. Without loss of generality assume $Va<Vb$, then

$$\begin{aligned} Va &= V(a+b-b) \\ &\geq \min\{V(a+b),Vb\} \\ &> Va \end{aligned}$$

which is a contradiction.

∎

4.3.3 *Definition* Two elements $a,b\varepsilon R$ are said to be *equivalent in V* denoted $a\sim b$ (in V), if $V(a-b)>Va$.

Note: $a\sim b$ implies $Va=Vb$ by the strong triangle law.

4.3.4 *Lemma* "$\sim$" is an equivalence relation on R.

Proof

(i) $a\sim a$ since $V(0) = V(a-a) > V(a)$ for all $a\varepsilon R$.

(ii) $a\sim b$ $b\sim a$. By lemma 4.3.1 and the strong triangle law, $a\sim b$ implies

$$V(b-a)=V(a-b)>Va=Vb$$

hence $b\sim a$.

(iii) $a\sim b$ and $b\sim c \rightarrow a\sim c$. $a\sim b$ and $b\sim c$ implies

$$\begin{aligned} V(a-c) &= V(a-b+b-c) \\ &\geq \min\{V(a-b),V(b-c)\} \\ &> \min\{Va,Vb\} \\ &= Va \end{aligned}$$

hence $a \sim c$.

∎

4.3.5 *Definition* An element $b \varepsilon R$ is said to be *equivalence-divisible* by an element $a \varepsilon R$ in V if there is an element $c \varepsilon R$ such that $b \sim ac$ (in V).

4.3.6 *Theorem* If R is an integral domain then V may be extended to the field of quotients of R by defining

$$V(a/b)=Va-Vb$$

Proof. We need only check the triangle law and the product law.

(i) Suppose without loss of generality that $V(a/b)<V(c/d)$. Then $Va-Vb<Vc-Vd \rightarrow Vad<Vbc$. Now

$$\begin{aligned} V(a/b+c/d) &= V((ad+bc)/bd) \\ &\geq \min\{V(ad),V(bc)\}-V(bd) \\ &= V(ad)-V(bd) \\ &= V(a/b) \end{aligned}$$

(ii) Product Law. $$\begin{aligned} V((ac)/(bd)) &= V(ac) - V(bd) \\ &= Va - Vb + Vc - Vd \\ &= V(a/b) + V(c/d) \end{aligned}$$

∎

4.3.7 *Definition* When R is a field, then the set $Va<\infty$ is an additive group Γ called the *value-group of V.*

4.3.8 *Definition* If the set $\Gamma^+ \equiv \{V a \in \Gamma \mid V a > 0\}$ has a minimum v, then V is said to be *discrete*. Γ then is a cyclic group generated by v. If V is a value on $\mathcal{Q}$, then Γ is isomorphic to Z.

4.4 AUGMENTED VALUES

Given a value V on $\mathcal{Q}$we would like to construct all values on the ring $\mathcal{Q}[x]$.

4.4.1 *Theorem* If V_0 is a value on $\mathcal{Q}$ and $\mu_1$is a real number, then the mapping

$$V_1 : \mathcal{Q}[x] \to R$$

defined by

$$V_1 f(x) = \min_i \{V_0 a_i + i\mu_1\}$$

where $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$, is a value on $\mathcal{Q}[x]$.

Proof. Only the triangle and product laws need be shown for V_1.

(i) Triangle Law. Let

$$f(x) = a_m x^m + \ldots + a_0$$

and $$g(x) = b_n x^n + \ldots + b_0,$$

then $$V_1(f+g) = \min_i \{V_0(a_i+b_i) + i\mu_1\}$$

$$\geq \min_i \{\min\{V_0 a_i, V_0 b_i\} + i\mu_1\}$$

$$\geq \min_i \{V_0 a_i + i\mu_1, V_0 b_i + i\mu_1\}$$

$$= \min\{\min_i\{V_0 a_i + i\mu_1\}, \min_i\{V_0 b_i + i\mu_1\}$$

$$= \min\{V_1 f, V_1 g\}$$

(ii) Product Law. Suppose $f(x) = a_m x^m$ and $g(x) = b_n x^n + \ldots + b_0$. Then

$$\begin{aligned} V_1(fg) &= V_1\Big(\sum a_m b_i x^{i+m}\Big) \\ &= \min_i\{V_0(a_m b_i) + (i+m)\mu_1\} \\ &= V_0 a_m + m\mu_1 + \min_i\{V_0 b_i + i\mu_1\} \\ &= V_1 f + V_1 g \end{aligned}$$

Hence by repeated use of the triangle law

$$V_1(fg) \geq V_1 f + V_1 g .$$

To see that equality holds, let j and k be the highest powers of x such that

$$V_1 f = V_1(a_j x^j)$$

and $$V_1 g = V_1(b_k x^k)$$

respectively. Then

$$V_0 a_{j+i} + (j+i)\mu_1 > V_0 a_j + j\mu_1 \qquad i \in Z^+$$

and $$V_0 b_{k-i} + (k-i)\mu_1 \geq V_0 b_k + k\mu_1 \qquad i \in Z^+$$

hence $$\begin{aligned} V_0 a_{j+i} + V_0 b_{k-i} + (j+k)\mu_1 &= V_0(a_{j+i} b_{k-i}) + (j+k)\mu_1 \\ &> V_0(a_j + b_k) + (j+k)\mu_1 \end{aligned}$$

which implies $V_0(a_{j+i} b_{k-i}) > V_0(a_j b_k)$.

hence by the strong triangle law

$$V_0\Big(\sum_{s+t=j+k} a_s b_t\Big) = V_0(a_j b_k)$$

i.e.

$$V_1(fg) = V_1 f + V_1 g$$

∎

4.4.2 *Definition* The value V_1 obtained in Theorem 4.4.1 is called a *first stage value* and is denoted

$$V_1 = [V_0, V_1 x=\mu_1] .$$

4.4.3 *Definition* A non-zero polynomial $\phi(x)\varepsilon Q[x]$ is said to be a *key polynomial over a value V* of $Q[x]$ if:

(i) whenever a product $f(x)g(x)$ is equivalence-divisible by $\phi(x)$ in V, then either $f(x)$ or $g(x)$ is equivalence-divisible by $\phi(x)$ in V,

(ii) any non-zero polynomial in $Q[x]$ equivalence-divisible by $\phi(x)$ in V has degree in x greater than or equal to the degree of $\phi(x)$,

(iii) $\phi(x)$ is monic.

When there is no ambiguity, $\phi(x)$ will be abbreviated by ϕ. This convention will also apply to other polynomials.

4.4.4 *Theorem* If ϕ is a key-polynomial over a value V on $Q[x]$, then ϕ is irreducible in $Q[x]$.

Proof. Suppose $\phi=fg$. Then by 4.4.3*(i)* either f or g is equivalence-divisible by ϕ in V. Suppose f is, then by 4.4.3*(ii)* $\deg f \geq \deg\phi \rightarrow \deg f = \deg\phi$, that is ϕ is irreducible in $Q[x]$. ∎

If $f(x)\varepsilon\mathcal{Q}[x]$ then there exist polynomials $q_0(x)$ and $f_0(x)$ in $\mathcal{Q}[x]$ such that

$$f(x) = q_0(x)\phi + f_0(x)$$

where $f_0(x)=0$ or $\deg f_0<\deg\phi$. $q_0(x)$ can again be represented

$$q_0(x) = q_1(x)\phi + f_1(x)$$

where $f_1(x)=0$ or $\deg f_1<\deg\phi$. Continuing in this manner yields the *canonical expansion of f(x) in* ϕ.

$$(1) \qquad f(x) = f_m(x)\phi^m + \ldots + f_1(x)\phi + f_0(x)$$

where $f_i(x)=0$ or $\deg f_i<\deg\phi$.

In the future a representation of a polynomial f(x) of the form (1) will always be the canonical expansion of f(x) in ϕ.

If V is a value on $\mathcal{Q}[x]$ and ϕ is a key polynomial over V, then a new value W on $\mathcal{Q}[x]$ can be obtained by assigning to ϕ a value $\mu>V$ and defining

$$(2) \qquad Wf = \min_i\{Vf_i+i\mu\}$$

where the f_i are the coefficients of the representation of f(x) in ϕ.

To see that W is, in fact, a value on $\mathcal{Q}[x]$ the following Lemma will be required.

4.4.5 *Lemma* If ϕ is a key polynomial over a value V of $\mathcal{Q}[x]$ and f(x) is a non-zero polynomial in $\mathcal{Q}[x]$ such that

$$f(x) = q(x)\phi + f(x)$$

where $r(x)=0$ or $\deg r<\deg\phi$, then

(i) $Vr \geq Vf$

(ii) $Vr>Vf$ iff f is equivalence-divisible by ϕ in V.

(iii) $V(q\phi)\geq Vf$.

Proof. *(i)* Suppose $Vr<Vf$, then $V(r=q\phi)=Vf>Vr \rightarrow r \sim q\phi$ (in V) $\rightarrow \deg r \geq \deg\phi$ but this is a contradiction.

(ii) Suppose $Vr>Vf$, then $V(f-q\phi)=Vr>Vf \rightarrow f$ is equivalence-divisible by ϕ in V. Conversely if f is equivalence-divisible by ϕ in V then there exist polynomials $s(x)$ and $t(x)$ such that $f(x) = s(x)\phi + t(x)$ and $Vt>Vf$. Now if $Vr=Vf$ then $r(x) = f(x) - q(x)\phi = (s(x)-q(x))\phi + t(x)$ where $Vt>Vr$ which implies that $r(x)$ is equivalence-divisible by ϕ in V which is a contradiction.

(iii)
$$\begin{aligned} V(q\phi) &= V(f-r) \\ &\geq \min\{Vf, Vr\} \\ &= Vf. \end{aligned}$$

■

4.4.6 *Theorem* If V is a value on $Q[x]$, ϕ is a key polynomial over V and $\mu>V$ is a real number, then the mapping (2)

$$Wf = \min_i\{Vf_i + i\mu\}$$

is a value of $Q[x]$.

Proof. Only the triangle and product laws need be shown.

(i) Triangle Law

$$\begin{aligned} W(f+g) &= \min_i\{V(f_i+g_i)+i\mu\} \\ &\geq \min_i\{\min\{Vf, Vg\}+i\mu\} \end{aligned}$$

$$\geq \min_i\{Vf_i+i\mu, Vg_i+i\mu\}$$

$$= \min\{\min_i\{Vf_i+i\mu\}, \min_i\{Vg_i+i\mu\}\}$$

$$= \min\{Wf, Wg\}$$

(ii) Product Law

Consider first two expansions of the form $a(x)\phi^s$ and $b(x)\phi^t$. Then $a(x)b(x) = c(x)\phi + d(x)$. Now $a(x)b(x)$ is not equivalence-divisible by ϕ in V for if it were, then either $a(x)$ or $b(x)$ would also be. Hence by Lemma 4.4.5 $Vd=V(ab)$ and

$$V(c(x)\ ) = V(a(x)b(x)-d(x))$$

$$\geq V(ab)$$

$$= Vd$$

Now

$$V(c(x)\phi) = Vc + V\phi$$

$$< Vc + \mu$$

which implies $Vc + \mu > V(ab) + Vd$ which then implies

$$W(a(x)\phi^s b(x)\phi^t) = W(c(x)\phi^{s+t+1} + d(x)\phi^{s+t})$$

$$= \min\{Vc+(s+t+1)\mu,\ Vd+(s+t)\mu\}$$

$$= Vd + (s+t)\mu$$

$$= V(ab) + (s+t)\mu$$

$$= Va+s\mu + Vb+t\mu$$

$$= W(a(x)\phi^s) + W(b(x)\phi^t)$$

which establishes the product law for monomials in ϕ. By use of the triangle law and repeated applications of the product law for monomials, we have $W(fg)\geq Wf+Wg$.

Now let s and t denote the largest integers such that

$$Wf = W(f_s(x)\phi^s)$$

and

$$Wg = W(g_t(x)\phi^t)$$

then as in Theorem 4.4.1

$$W(fg) = W(f_s(x)\phi^s) + W(g_t(x)\phi^t)$$

$$= Wf + Wg$$

∎

4.4.7 *Definition* A value W obtained from a value V on $Q[x]$ is called an *augmented value* of V and is denoted

$$W = [V, W\phi=\mu]$$

4.5 PROPERTIES OF AUGMENTED VALUES

4.5.1 *Theorem (monotonicity)* An augmented value W of V has the property that for all non-zero polynomials f(x)

(1) $$Wf \geq Vf$$

Furthermore inequality holds iff f(x) is equivalence-divisible by ϕ in V. If the degree of f(x) is less than the degree of ϕ then equality holds.

Proof. Let $f(x) = f_m\phi^m + \ldots + f_1\phi + f_0$. If m=0 then Wf=Vf by definition. Now make the inductive hypothesis that the theorem is true for all polynomials of degree m-1 or less in ϕ. Then $f(x) = q(x)\phi + f_0(x)$ where $q(x) = f_m\phi^{m-1} + \ldots + f_1(x)$.

By the inductive hypothesis $Wq \geqq Vq$, hence

$$W(q\ ) = Wq + W\phi$$

$$\geqq Vq + V\phi$$

$$= V(q\phi)$$

$$\geqq Vf$$

by Lemma 4.4.5*(iii)*. But $Wf_0 = Vf_0 \geqq Vf$ by Lemma 4.4.5*(ii)* hence

$$Wf = \min\{W(q\phi), Wf_0\} \geqq Vf.$$

This establishes the first claim.

Now $Vf_0 = Wf_0 \geqq Wf \geqq Vf$ hence if inequality holds in (1), then $Vf_o > Vf$ and f is equivalence-divisible by ϕ in V. Conversely if f is equivalence-divisible by ϕ in V then

$$Wf \geqq \min\{W(q\phi), Wf_o\}$$

$$\geqq \min\{V(q\phi), Vf_o\}$$

$$> Vf$$

and the second claim is established.

Finally if $\deg f < \deg \phi$, then $f = f_0 \rightarrow Wf = Vf_0$ by definition.

∎

4.6 INDUCTIVE VALUES

4.6.1 *Definition* Let $V = [V_0, V_1 x=\mu_1]$ be a first stage value on $\mathcal{Q}[x]$. Then a k^{th} *stage inductive value* V_k is the augmented value obtained from a sequence of values $V_0, V_1, \ldots V_{k-1}, V_k$ where

$$V_i = [V_{i-1}, V_i\phi_i=\mu_i] \quad (i=2,3,\ldots,k)$$

such that

(i) $\deg\phi_i \geq \deg\phi_{i-1}$

(ii) ϕ_i is not equivalent to ϕ_{i-1} in V_{i-1}

Note: (1) the first key polynomial is always $\phi_1=x$

(2) $\mu_i = V_i\phi_i > V_{i-1}\phi_{i-1} = \mu_{i-1}$

The value V_k will be denoted

$$V_k = [V_0, V_1 x=\mu_1, V_2\phi_2=\mu_2, \ldots, V_k\phi_k=\mu_k].$$

4.6.2 *Definition* Given a sequence $\{V_k\}$ of inductive values, the *limit-value* V_∞ is defined to be

$$V_\infty f = \lim_{k\to\infty} V_k f .$$

By the monotonicity of inductive values, $V_\infty f = \infty$ if it is not finite. The following theorem establishes that V_∞ is a value on $\mathcal{Q}[x]$.

4.6.3 *Theorem* If V_∞ is a limit-value obtained from a sequence of inductive values $\{V_k\}$, then V_∞ is a value on $\mathcal{Q}[x]$.

Proof. Only the triangle and product laws need be shown.

(i) Triangle Law: If $V(f+g)=\infty$ then

$$V_\infty(f+g) \geq \min\{V_\infty f, V_\infty g\} .$$

Suppose $V_\infty(f+g) < \infty$. Then $V_\infty f < \infty$ and $V_\infty g < \infty$. For if not then we can assume $V_\infty f = \infty$. But this implies that there is a natural number k such that

$$V_k f > V_\infty(f+g) \geq V_k(f+g) = V_k g .$$

Hence $V_k(f+g) = V_k f > V_\infty(f+g)$ which is a contradiction. Therefore assume, without loss of generality, that $V_\infty g \leq V_\infty f < \infty$. Now if $V_\infty(f+g) < V_\infty g$ and $V_\infty(f+g) < V_\infty f$, then there is a positive integer N such that for all $k \geq N$, $V_\infty(f+g) < V_k g$ and $V_\infty(f+g) < V_k f$, that is

$$V_\infty(f+g) < \min\{V_k f, V_k g\} .$$

But $$\min\{V_k f, V_k g\} \leq V_k(f+g) \leq V_\infty(f+g) .$$

Therefore either $V_\infty f \geq V_\infty(f+g)$ or $V_\infty g \geq V(f+g)$.
In either case

$$\min\{V_\infty f, V_\infty g\} \leq V_\infty(f+g) .$$

(ii) Product Law:

$$V_\infty(fg) = \lim V_k(fg)$$

$$= \lim V_k f + \lim V_k g$$

$$= V_\infty f + V_\infty g .$$

■

In the construction of an inductive value V_k, the only requirement made is that $\deg\phi_i \geq \deg\phi_{i-1}$ $(i=1,2\ldots,k)$. When several successive key polynomials have the same degree, the following Lemma will be required.

4.6.4 *Lemma* If, for the inductive value V_s, the key polynomials $\phi_{s+1}, \ldots, \phi_t$ all have the same degree, then for $s<j<t$,

(i) $V_s(\phi_{j+1}-\phi_j) = \mu_j$

(ii) $V_s\phi_{s+1} = V_s\phi_{s+2} = \ldots = V_s\phi_{t-1} = V_s\phi_t$

Proof. *(i)* For $(j=s+1,\ldots,t-1)$ let $s_j(x) = \phi_{j+1}(x)-\phi_j(x)$. Then $\deg s_j < \deg\phi_j$ since each key polynomial is monic. By Theorem 4.5.1

$$V_s s_j(x) = V_{s+1} s_j(x) = \ldots = V_t s_j(x)$$

in particular

$$\begin{aligned} V_s s_j(x) &= V_{j+1} s_j(x) \\ &\geq \min\{V_{j+1}\phi_{j+1}, V_{j+1}\phi_j\} \\ &\geq \min\{V_{j+1}\phi_{j+1}, V_j\phi_j\} \\ &= \mu_j \end{aligned}$$

which implies $V_s s_j(x) = \mu_j$ since otherwise

$$V_s s_i(x) = V_j(\phi_{j+1}-\phi_j) > \mu_j = V_j\phi_j$$

which implies $\phi_{j+1} \sim \phi_j$ in V_j which is a contradiction.

(ii) By Theorem 4.5.1 $V_i\phi_j > V_{j-1}\phi_j \rightarrow V_s s_j = \mu_j > V_{j-1}\phi_j$

but $V_{j-1}\phi_j \geq V_s\phi_j$ hence by the strong triangle law,

$$V_s\phi_{j+1} = \min\{V_s s_j, V_s\phi_j\} = V_t\phi_j$$

which implies

$$V_s\phi_{s+1} = V_s\phi_{s+2} = \ldots = V_s\phi_t .$$

∎

4.6.5 *Theorem* If the i^{th} stage of an inductive value

$$V_k = [V_0, V_1 x=\mu_1, V_2\phi_2=\mu_2, \ldots, V_k\phi_k=\mu_k]$$

uses a key polynomial ϕ_i with assigned value $V_i\phi_i=\mu_i$, then for $i \leq k$,

$$V_k\phi_i = V_i\phi_i = \mu_i .$$

Proof. If $\deg\phi_k > \deg\phi_i$, then the theorem holds by Theorem 4.5.1. So suppose $\deg\phi_k = \deg\phi_{k-1} = \ldots = \deg\phi_i$. Write

$$\phi_i = \phi_k - s_{k-1} - s_{k-2} - \ldots - s_i ,$$

then

$$\begin{aligned} V_{k\,i} &= \min\{V_k\phi_k, V_k s_{k-1}, \ldots, V_k s_i\} \\ &= \min\{V_k\phi_k, V_{i-1} s_{k-1}, V_{i-1} s_{k-2}, \ldots, V_{i-1} s_i\} \\ &= \min\{\mu_k, \mu_{k-1}, \ldots, \mu_i\} \\ &= \mu_i . \end{aligned}$$

Note: equality holds because of the strong triangle law.

∎

4.6.6 *Theorem* Let V be the limit-value determined by the sequence of inductive values $\{V_k\}$. Then for a fixed non-zero polynomial f(x), either

(1) $$V_{k+1}f > V_k f \qquad (k=1,2,\ldots)$$

or there exists an integer N such that for i<N

(2) $$V_1 f < V_i f < V_N f = V_{N+1} f = \ldots = V_{N+j} f = \ldots$$

If (2) holds then there is a polynomial r(x) such that $\deg r < \deg \phi_{N+1}$ and $f \sim r$ in V_{N+j} $(j=1,2,\ldots)$.

Proof. Suppose (1) does not hold. Let N be the least positive integer such that

(3) $$V_N f = V_{N+1} f.$$

Write $f(x) = q(x)\phi_{N+1} + r(x)$. Then by Theorem 4.5.1,(3) implies that f is not equivalence-divisible by ϕ_{N+1} in V_N, hence by Lemma 4.4.5, $V_N r = V_n f$. Therefore for $k \geq N+1$

$$V_k(f-r) \geq V_{N+1}(f-r) = V_{N+1}(q\phi_{N+1})$$

$$> V_N(q\phi_{N+1})$$

$$\geq V_N f = V_N r = V_k r$$

Which implies $f \sim r$ in V_k, $k \geq N+1 \rightarrow V_k f = V_k r = V_N r = V_N f$ and (2) holds.

∎

4.6.7 *Definition* If V_k is an inductive value on $Q[x]$then by Theorem 4.3.6, V_k can be extended to a value on $Q(x)$ with value group Γ_k. Γ_k is called the *value group associated with* V_k.

4.6.8 *Theorem* Le V_k be an inductive value on $Q(x)$. Then Γ_k is the additive group

$$Z[1,\mu_1, \ldots ,\mu_k].$$

Proof. Clearly $\Gamma_k \subseteq Z[1, \mu_1, \ldots , \mu_k]$. By Theorem 4.6.5 if $m = m_0+m_1\mu_1+ \ldots +m_k\mu_k \in Z[1, \mu_1, \ldots , \mu_k]$ then $f(x) = bx^{m_1}{}_2{}^{m_2}\ldots{}_k{}^{m_k} \in Q(x)$ and $V_k f = m \quad Z[1, \mu_1,\ldots, \mu_k] \subseteq \Gamma_k$

■

4.6.9 *Definition* A real number $\mu$is said to be *commensurable* with a value group Γ if there is an integer n such that $n\mu \in \Gamma$.

4.6.10 *Theorem* If V_k is an inductive value then for $0<i<k$, μ_i is commensuralbe with Γ_{i-1}.

Proof. Let $\phi_{i+1} = f_m\phi_i^m+ \ldots +f_0$ be the canonical expansion of ϕ_{i+1} in ϕ_i and suppose μ_i is not commensurable with Γ_{i-1}. Then

$$V_i(f_j\phi_i^j) \neq V_i(f_k\phi_i^k) \quad (j=k)$$

since otherwise

$$(k-j)\mu_i = V_i f_j - V_i f_k \in \Gamma_{i-1}.$$

Let j be the term such that $v_i\phi_{i+1} = V_i(f_j\phi_i^j)$, then

$$V_i(\phi_{i+1} - f_j\phi_i^j) > V_i\phi_{i+1}$$

which implies $\phi_{i+1} \sim f_j\phi_i^j$ (in V_i) but this implies that either f_j or ϕ_i is equivalence-divisible by ϕ_{i+1} in V_i. Since $\deg f_i < \deg\phi_i \leq \deg\phi_{i+1}$, $f_j(x)$ cannot be equivalence-divisible by ϕ_{i+1} in V_i

If ϕ_i were equivalence-divisible by ϕ_{i+1} in V_i then $\deg\phi_i = \deg\phi_{i+1}$ and so

$$\phi_{i+1} = \phi_i + (\phi_{i+1} - \phi_i)$$

and $$V_i(\phi_{i+1} - \phi_i) > V_i\phi_i$$

which implies $\phi_i \sim \phi_{i+1}$ in V_i which is a contradiction. Hence μ_i is commensurable with Γ_{i-1}.

∎

4.7 THE FINITENESS CRITERION

4.7.1 *Definition* A sequence of polynomials $\{f_n\}$ in $Q[x]$ is said to be a *W-Cauchy sequence* if for any real number ν, there exists an integer N such that

$$W(f_n - f_m) > \nu \quad \text{for all } n, m \geq N.$$

The ring $Q[x]$ can be completed with respect to a value W by the usual method. Since it will always be clear what value $Q[x]$ is completed with respect to, the completion will be denoted by $\overline{Q[x]}$. Then $f \varepsilon \overline{Q[x]}$ is said to be a *W-limit* of a W-Cauchy sequence $\{f_n\}$ in $Q[x]$ if $\lim_{n\to\infty} W(f - f_n) = \infty$

4.7.2 *Theorem (Finiteness Criterion)* Let V_∞ be the limit-value of the inductive sequence $\{V_k\}$over key polynomials ϕ_k of constant degree M for $k>t>0$ for some positive integer t. Let $\overline{Q[x]}$ be the completion of $Q[x]$ with respect to V_t. Then

(i) $\{\phi_t\}$ is a V_t-Cauchy sequence and hence has a V_t-limitϕ in $\overline{Q[x]}$.

(ii) V_∞ is finite iff there is no non-zero polynomial f(x) divisible by ϕin $\overline{Q[x]}$.

Proof. *(i)* By Theorem 4.6.10 each μ_i is commensurable with the value group Γ_{i-1} of V_{i-1}. Since Γ_0 is discrete, Γ_t is discrete by induction. By Lemma 4.6.4

$$V_t(\phi_{i+1} - \phi_i) = \mu_i \in \Gamma_t \qquad (i>t)$$

hence

$$\Gamma_i = \Gamma_t \qquad (i>t)$$

but $\{\mu_i\}$ is a monotone strictly increasing sequence in Γ_t which implies $\lim\mu_i = \infty$. By the strong triangle law

$$V_t(\phi_{i+j} - \phi_i) = V_t\left(\sum_{k=1}^{i+j-1} (\phi_{k+1} - \phi_k)\right)$$

$$= \min_k\{\mu_k\} = \mu_i.$$

Hence $\{\phi_k\}$ is a V_t-Cauchy sequence and has a V_t-limit ϕ in $\overline{Q[x]}$.

(ii) Suppose now that $f(x)\neq 0$ is divisible by ϕ in $\overline{Q[x]}$. Then $f(x) = h$ where $h\neq 0$ is a V_t-limit of a Cauchy sequence $\{h_i\}$ in $Q[x]$. We then have $\lim_{i\to\infty} V_t(f-h_i\phi_i) = \infty$. Since $\lim_{i\to\infty} V_t h_i = V_t h \neq 0$, $\{V_t h_i\}$ is eventually constant which implies

$$\lim_{i\to\infty} (V_t h_i + \mu_i) \to \infty.$$

Now for $i>t$

$$V_i f \geq \min\{V_i(h_i\phi_i), V_i(f-h_i\phi_i)\}$$

$$\geq \min\{V_t h_i + \mu_i, V_t(f-h_i\phi_i)\}$$

Taking the limit as $i\to\infty$ yields

$$V_\infty f = \lim V_i f = \infty$$

and V_∞ is not finite.

Conversely suppose that V_∞ is not finite, then for some $g(x)\neq 0$, $V_\infty g = \infty$. Now for $i>t$ write $g = q_i\phi_i + r_i$ where $r_i=0$ or $\deg r_i < \deg\phi_i = M$. Using Theorem 4.5.1 and Lemma 4.4 6 yields

$$V_t(g - q_i\phi_i) = V_t r_i$$

$$= V_{i-1} r_i$$

$$\geq V_{i-1} g \to \infty$$

hence g is a V_t-limit of $\{q_i\phi_i\}$. Since $\phi_i\to\phi$ in V_t, then by the standard limit argument, $\{q_i\}$ converges to q in $\overline{Q[x]}$, and $g(x) = q(x)\phi$ and ϕ is a divisor of $g(x)$ in $\overline{Q[x]}$.

■

4.8 COMPLETENESS

4.8.1 *Theorem* Every non-Archimedean value W on the ring $\mathbb{Q}[x]$ can be represented either as an inductive value or as a limit-value.

Proof. We shall construct a sequence of inductive values $\{V_k\}$ with the following properties:

(i) $Wf \geq V_k f$ for all $f(x) \in \mathbb{Q}[x]$

(ii) if $\deg f < \deg \phi_k$, then $Wf = V_k f$

(iii) $W\phi_i = V_k \phi_i \qquad (i=1,2, \ldots ,k)$

Let $V_0 a = Wa$ for all rationals a and define $V_1 x = Wx = \mu_1$. Then *(i)* holds for k=1 since

$$\begin{aligned} Wf &\geq \min_i \{W(a_i x^i)\} \\ &= \min_i \{Wa_i + iWx\} \\ &= \min_i \{V_0 a_i + i\mu_i\} \\ &= V_1 f. \end{aligned}$$

Properties *(ii)* and *(iii)* hold by definition.

Suppose now that an inductive value V_k has been constructed with the three properties and that there exists a non-zero polynomial g(x) such that $Wg > V_k g$. Let $\psi(x)$ be a non-zero polynomial of least degree such that $W\psi > V_k \psi$. Without loss of generality $\psi(x)$ can be taken to be monic.

Let f(x) be any other non-zero polynomial such that $Wf > V_k \psi$ and write $f = q\psi + r$ where $r(x) = 0$ or $\deg r < \deg \psi$.

Then $V_k(f-q\psi) = W(f-q\psi)$

$\geq \min\{Wf, W(q\psi)\}$

$> \min\{V_k f, V_k(q\psi)\}$

which implies that f is equivalence-divisible by in V_k.

Conversely suppose f is equivalence-divisible by ψ in V_k. Then there exist polynomials q(x) and r(x) such that $f = q\psi + r$ and $V_k r > V_k f = V_k(q\psi)$. Then

$Wf \geq \min W(q\ ), Wr$

$\geq \min V_k q + W\ , V_k r$

$> V_k(q\ )$

$= V_k f.$

Hence $Wf > V_k f$ iff f is equivalence-divisible by ψ in V_k.

Now suppose f(x)g(x) is the product of two polynomials which are equivalence-divisible by ψ in V_k. Then

$Wf + Wg = W(fg) > V_k(fg) = V_k f + V_k g$

but by the inductive hypothesis $Wf \geq V_k f$ and $Wg \geq V_k g$ hence either $Wf > V_k f$ or $Wg > V_k g$, that is either f is equivalence-divisible by ψ in V_k or g is. Therefore by the construction of ψ, ψ is a key polynomial over the value V_k. Let $\phi_{k+1} = \psi$ and $\mu_{k+1} = W\psi > V_k\psi$. By *(iii)* and the inductive hypothesis, $W\phi_k = V_k\phi_k$, hence by the construction of ϕ_{k+1}, $\deg\phi_{k+1} \geq \deg\phi_k$. ϕ_{k+1} is not equivalence-divisible by ϕ_k in V_k since, if it

were, then by the equivalence-irreducibility of ϕ_{k+1}, $\phi_{k+1} \sim \phi_k$ and thus $V_k(\phi_k - \phi_{k+1}) > V_k\phi_k = V_k\phi_{k+1}$ which implies

$$W\phi_k \geq \min\{W\phi_{k+1}, W(\phi_k - \phi_{k+1})\}$$

$$> \min\{V_k\phi_{k+1}, V_k(\phi_k - \phi_{k+1})\}$$

$$= V_{k\ k} = W_k$$

which is a contradiction. Thus $V_{k+1} = [V_k, V_{k+1}\phi_{k+1} = \mu_{k+1}]$ is an inductive value.

Now *(i)* holds for V_{k+1} since

$$Wf \geq \min\{W(f_i\phi_{k+1}^i)\}$$

$$= \min\{Wf_i + i\mu_{k+1}\}$$

$$= \min\{V_k f_i + i\mu_{k+1}\}$$

$$= V_{k+1}\ f$$

and *(ii)* and *(iii)* hold by the construction of ϕ_{k+1}. Therefore either W is an inductive value V_k or there is an inductive sequence $\{V_k\}$ satisfying *(i)*, *(ii)* and *(iii)*.

Suppose W is not an inductive value. Then by the conditions $Wf \geq V_\infty f = \lim V_k f$ for all f. But $Wf \nmid V_k f$ for suppose that inequality held. Then since $V_k f$ is monotone increasing, $Wf > V_k f$ for $k \in Z^+$ hence f is equivalence-divisible by ϕ_{k+1} in V_k for all k, and by Theorem 4.5.1 $V_{k+1} f > V_k f$. But this cannot hold if the degrees of ϕ_k increase indefinitely, hence there is a $t \in Z^+$ such that for $k > t$, $\deg\phi_k =$

constant = M. As in the proof of the Finiteness Criterion, the monotonic increasing sequence $\{V_k f\}$ consists of numbers in the discrete value group Γ_t and

$$Wf \geq V_\infty f = \lim V_k f = \infty$$

but this can hold only for $f(x) = 0$, hence $Wf = V_\infty f$.

∎

4.9 PROPERTIES OF KEY POLYNOMIALS

4.9.1 *Lemma* Let V_k be an inductive value ($k>1$), if for a polynomial $b(x)$, $V_k b = V_{k-1} b$, then there is a polynomial $b'(x)$ such that $bb' \sim 1$ (in V_k) and $V_k b' = V_{k-1} b'$.

Proof. By hypothesis $b(x)$ is not divisible by ϕ_k. Since ϕ_k is irreducible in the ordinary sense, there exists polynomials $b'(x)$ and $c(x)$ such that

$$b'(x)b(x) + c(x)\phi_k(x) = 1$$

and where $\deg b' < \deg \phi_k$. Now $V_k(c\phi_k) > V_{k-1}(c\phi_k)$ implies

$$\begin{aligned} V_k(bb'-1) &= V_k(c\phi_k) \\ &> V_{k-1}(c\phi_k) \\ &= \min\{V_{k-1}bb', V_{k-1}1\} \\ &= \min\{V_k bb', V_k 1\} \end{aligned}$$

hence $bb' \sim 1$ (in V_k). Since $\deg b' < \deg \phi_k$, $V_k b' = V_{k-1} b'$.

∎

4.9.2 *Lemma* In any inductive value V_k, the key polynomial ϕ_k is equivalence-irreducible in V_k. A polynomial f(x) not equivalence-divisible by ϕ_k in V_k has a value $V_k f$ in Γ_{k-1}.

Proof. A polynomial $f(x) = \sum f_i(x) \phi_k^i$ is equivalence-divisible by ϕ_k in V_k iff $V_k f_0 > V_k f$. Therefore if f(x) is not equivalence-divisible by ϕ_k in V_k, then $V_k f = V_k f_0 = V_{k-1} f_0$ and $V_k f \varepsilon \Gamma_{k-1}$.

∎

4.9.3 *Definition* An inductive value V_k is said to be *commensurable* if μ_k is commensurable with the value-group Γ_{k-1}. If V_k is commensurable, there is a smallest positive integer τ_k such that $\tau_k \mu_k \varepsilon \Gamma_{k-1}$.

4.9.4 *Lemma* If V_k is a commensurable inductive value, then for any real number $\lambda \varepsilon \Gamma_k$, there is a polynomial $R_\lambda(x)$ such that $V_k R_\lambda = \lambda$ and such that if V_{k+1} is an arbitrary augmented value of V_k, then $V_{k+1} R_\lambda = \lambda$.

Proof. Let $\lambda = m_0 + m_1 \mu_1 + \ldots + m_k \mu_k$ where m_i are arbitrary integers. Since each μ_i is commensurable with the previous value group Γ_{i-1}, each is commensurable with $\Gamma_0 = Z$. Therefore we can take m_i to be non-negative integers. Define $R_\lambda(x) = a \| \phi_i(x)^{m_i}$ where $V_0 a = m_0$. Then $V_k R_\lambda = \lambda$ and $V_{k+1} R_\lambda = \lambda$ for any augmented value V_{k+1}.

∎

4.9.5 *Theorem* A polynomial f(x) is a key polynomial for an inductive value V_k iff the following conditions hold.

(i) In the canonical expansion of f(x) in ϕ_k, $V_k f = V_k f_0$,

(ii) $f_m(x) = 1$, $V_k \phi_k^m = V_k f$ and $m \equiv 0 \pmod{\tau_k}$,

(iii) f(x) is equivalence-irreducible in V_k

Proof. Suppose f(x) is a key polynomial over V_k. Then *(iii)* holds by definition.

(i) Suppose $V_k f_0 > V_k f$, then $V_k(f - q\phi_k) = V_k f_o > V_k f$ which implies $f \sim q\phi_k$ in V_k but this is a contradiction since $\deg q < \deg f$, hence $V_k f = V_k f_0$.

(ii) Suppose $f_m(x) \neq 1$, then since $V_k f_m = V_{k-1} f_m$, there exists a polynomial b'(x) such that $b'f \sim 1$ (in V_k). The polynomial b'f has degree $n \cdot \deg\phi_k < \deg f$ and b'f is equivalence-divisible by f in V_k which contradicts Definition 4.4.3 *(ii)*. Hence f is monic in ϕ_k. Now $V_k \phi_k^m = V_k f$ since otherwise $f - \phi_k^m$ is a polynomial of degree less than the degree of f which is equivalent to f in V_k.

Finally $V_k \phi_k^m = V_k f = V_k f_0 = V_{k-1} f_0 \varepsilon \Gamma_{k-1}$ which implies that $n \equiv 0 \pmod{\tau_k}$.

Conversely suppose that *(i)*, *(ii)* and *(iii)* hold for some polynomial f(x). Then f(x) satisfies *(ii)* and *(iii)* of Definition 4.4.3. Clearly f is monic and any equivalence-multiple of f(x) must be of degree at least m in ϕ_k in V_k. Finally *(i)* of Definition 4.4.3 follows from condition *(iii)*.

∎

4.10 A EUCLIDEAN ALGORITHM IN V_k

4.10.1 *Definition* Let V_k be an inductive value with last key polynomial ϕ_k. If f(x) is a polynomial with canonical expansion $\sum f_i \phi_k^i$ in ϕ_k, then the *effective degree* of f(x) in ϕ_k, denoted $D_\phi f$, is the largest exponent i such that $V_k f = V_k(f_i \phi_k^i)$. From section 4.4 and the product law we have $D_\phi fg = D_\phi f + D_\phi g$.

4.10.2 *Definition* If $D_\phi f=0$ then f(x) is said to be an *equivalence-unit in* V_k.

4.10.3 *Definition* A polynomial e(x) is said to have an *equivalence-inverse in* V_k if there is a polynomial h(x) such that $eh \sim 1$ (in V_k)

4.10.4 *Lemma* A Polynomial e(x) is an equivalence-unit in V_k iff it has an equivalence-inverse in V_k.

Proof. If e(x) is an equivalence-unit in V_k, then $V_k e = V_{k-1} e$, hence by Lemma 4.9.1 there is a polynomial h(x) such that $eh \sim 1$ (in V_k) and $V_k h = V_{k-1} h$.

Conversely if e(x) has an equivalence-inverse h(x) in V_k, then

$$D_\phi eh = D_\phi e + D_\phi h = D_\phi 1 = 0$$

Since $D_\phi f \geq 0$ for all polynomials f(x), this implies that $D_\phi e = D_\phi h = 0$.

∎

4.10.5 *Lemma* Any polynomial f(x) can be represented $f \sim ea$ (in V_k) where e(x) is an equivalence-unit in V_k and a(x) is minimal. Furthermore a(x) and f(x) have the same equivalence-divisors.

Proof. Let $D_\phi f = \alpha$. Since $D_\phi f = 0$, there is a polynomial f'_α such that $f_\alpha f'_\alpha \sim 1$ (in V_k) by Lemma 4.10.4. In the canonical expansion of $f'_\alpha f$ in ϕ_k, delete all terms not of minimum value. Denote this new polynomial by a(x). Then a(x) is minimal and has an expansion in ϕ_k begining with ϕ_k^α, hence a(x) is monic. Clearly $f'_\alpha f \sim a$ (in V_k) hence $f \sim f_\alpha a$ (in V_k).

Finally an equivalence-divisor of f(x) is an equivalence-divisor of $f_\alpha(x)a(x)$ but since $f_\alpha(x)$ is an equivalence-unit, it must also be an equivalence-divisor of a(x).

∎

4.10.6 *A Euclidean Algorithm in V_k*

Let f(x) and g(x) be two polynomials such that $D_\phi f \geq D_\phi g$. Write $g \sim e_1 a_1$ by the preceeding Lemma. Then $f(x) = q(x)a_1 + r_2(x)$ and $D_\phi r_2 < D\, a_1$. If $V_k r_2 > V_k f$ then $a_1(x)$, and therefore g(x) is an equivalence-divisor of f(x). Otherwise $V_k r_k = V_k f$ since $a_1(x)$ is minimal, which implies $V_k f = V_k qa_1 = V_k r_2$. In this case we can repeat the process

$$r_2 \sim e_2 a_2 \quad (\text{in } V_k)$$

.

.

.

until a remainder d(x) is obtained where $V_k d > V_k f$. The

polynomial d(x) is then the greatest commom equivalence-divisor and

(1) $$d(x) \sim s(x)f(x) + t(x)g(x) \quad (\text{in } V_k)$$

for suitable polynomials s(x) and t(x).

4.10.7 *Theorem* In an inductive value V_k, every polynomial f(x) has a decomposition

(2) $$f(x) \sim e(x)\psi_1(x)\psi_2(x) \ldots \psi_n(x) \quad (\text{in } V_k)$$

where e(x) is an equivalence-unit and $\psi_i(x)$ is a key polynomial in V_k. Furthermore this decomposition is unique up to equivalence in V_k.

Proof. The representation (2) follows from (1). Since $\psi_i(x)$ are minimal, they satisfy the requirements to be a key polynomial in V_k.

∎

4.11 AN IRREDUCIBILITY CRITERION

4.11.1 *Theorem* Let V_k be an inductive value with last key polynomial ϕ_k. Then a polynomial $f(x) = \sum_{i=1}^{m} f_i(x)\phi_k^i$ is a key polynomial over V_k if the following conditions hold:

(i) $f_m(x) = 1$

(ii) $V_k f = V_{k\,k}^{\,i} = V_k f_0$

(iii) If $n<m$ is a positive integer, then $n\mu_k \nmid \Gamma_{k-1}$.

Proof. By Theorem 4.9.5 we need only show that f(x) is equivalence-irreducible in V_k. By Theorem 4.10.7

(1) $$f(x) \sim e(x)\prod\psi_i(x) \quad (\text{in } V_k)$$

where $\psi_i(x)$ are key polynomials in V_k. Each $\psi_i(x)$ has the form

$$\psi_i(x) = \phi_k^e + h_{e-1}\phi_k^{e-1} + \ldots + h_0$$

where $V_k\psi_i = V_k\phi_k^e = V_k h_0 \varepsilon \Gamma_{k-1}$. By the minimal condition *(iii)* of the hypothesis, e=km for some integer $k\varepsilon Z^+$. But since

$$m = \deg f \text{ in } \phi_k \geq \deg\psi_i \text{ in } \phi_k = e = km,$$

k=1, hence the degf in ϕ_k is equal to $\deg\psi_i$ in ϕ_k and there can only be one key polynomial ψ_i in the product (1). Therefore $f \sim e\psi$ (in V_k). Since ψ and f have the same equivalence-divisors, f is equivalence-irreducible and thus a key polynomial.

∎

4.11.2 *Corollary* If f(x) is a polynomial satisfying the conditions of Theorem 4.11.1 with respect to an inductive value V_k, then f(x) is irreducible.

Proof. By Theorem 4.11.1 f(x) is a key polynomial and thus, by Theorem 4.4.4, f(x) is irreducible.

∎

4.12 APPLICATIONS

4.12.1 *Schönemann's Theorem (1.2.1)* Let

$$V_2 = [V_o p=1,\ V_1 x=0,\ V_2\phi_2=1/m]$$

then for $f(x) = \phi_2^m + pf_0$, ϕ_2 is irreducible modulo p and hence a key polynomial over V_2. Since $V_2 f = V_2\phi_2^m = V_2(pf_0)$

$= V_1(pf_0) = V_0p + V_1f_0 = 1$, if $k<m$, then $k\mu_2 = k/m \notin \Gamma_o \equiv Z$. Hence f(x) is irreducible by Corollary 4.11.2.

∎

4.12.2 *Eisenstein's Theorem* (1.2.2) Let $V_1 = [V_0p=1, V_1x=1/n]$. Then for $f(x) = \sum_{i=0}^{n} a_i x^{n-i}$, the conditions of Theorem 1.2.2 imply that $V_1f = V_1(a_0x^n) = V_1x^n = nV_1x = 1$, since for $0<i<n$,

$$V_1(a_ix^{n-i}) = V_0a_i + (n-i)V_1x$$

$$\geq 1 + (n-i)/n$$

$$> 1$$

and finally $V_1a_n = V_0a_n = 1$. Clearly for $k<n$, $k/n \notin \Gamma_0 \equiv Z$. Hence f(x) is irreducible.

∎

4.12.3 *Königsberger's Theorem* (1.2.3) Let

$$V_1 = [V_0p=1/e, V_1x=1/n].$$

Then for $f(x) = x^n+a_1x^{n-1}+ \ldots + a_{n-1}x + a_n$, the conditions of Theorem 1.2.3 imply that

$$V_1f = V_1x^n = nV_1x = 1.$$

For $0<i<n$ $\quad V_1(a_ix^{n-1}) = V_0a_i + (n-i)V_1x$

$$\geq (1/e)(ie/n +1) + (n-i)/n$$

$$> i/n + (n-i)/n$$

$$= 1.$$

Finally $V_1 a_n = V_0 a_n = e(1/e) = 1$. Clearly for $k<n$, $k/n \notin \Gamma_0 \equiv Z[1,1/e]$ since $(e,n)=1$. Hence $f(x)$ is irreducible.

■

V. CONCLUSIONS

The three approaches to deciding the irreducibility of a polynomial $f(x)\varepsilon\mathcal{Q}[x]$ provide sufficient conditions for irreducibility.

Perron's method shows that a polynomial is irreducible provided there is a rational prime p which has just one ideal factor in $\mathcal{Q}[\xi]$ where $f(\xi)=0$. This is equivalent to showing that the prime p has just one ideal factor in the ring $\mathcal{Q}[x]/f(x)$. For example, Schönemann's Theorem 1.2.1, asserts the irreducibility of f(x) by showing that p has just one ideal factor $\mathfrak{p}=(p,\phi(x))$.

Dumas' approach is based on the observation that if a polynomial is p-adically irreducible, then it must also be irreducible over $\mathcal{Q}[x]$.

MacLane's work shows that both the approach of Perron and that of Dumas are simply statements about p-adic non-Archimedean values on $\mathcal{Q}[x]$. In two papers extending section IV, [13] and [14], MacLane shows that there is a 1:1 correspondence between k^{th} stage approximates V_k to f(x) arising from a p-adic value V_0 and the prime ideal factors of p in the ring of algebraic integers of $\mathcal{Q}[\xi]$ determined by f(x).

All these criteria are sufficient conditions for irreducibility and the quest for a necessary condition remains elusive.

BIBLIOGRAPHY

[1] Bachman, George, *Introduction to p-Adic Numbers and Valuation Theory*, Academic Press, 1972.

[2] Bauer, "Beitrag zur Theorie der irreduzibeln Gleichungen," *Journal für die Mathematik*, v. 128, p. 298-301, 1905.

[3] Bauer, "Verallgemeinerung eines Sätzes von Schönemann," *Journal für die Mathematik*, v. 128, p. 87-89, 1905.

[4] Dorwart, H. L., "Irreducibility of Polynomials," *The American Mathematical Monthly*, v. 32, p.369-381, June-July 1935.

[5] Dumas, M. G., "Sur quelques cas d'irréductibilité des Polynomes à Coefficients Rationnels," *Journal de Mathematiques Pures et Appliqués, Series 6*, v. 2, p. 191-258, 1906.

[6] Eisenstein, "Uber die Irreductibilität und einige andere Eigenschaften der Gleichung, von selcher die Theilung der ganzen lemniscate abhangt," *Journal für die Mathematik*, v. 39, p. 166, 1850.

[7] Hensel, " Neue Grundlagen der Arithmetik," *Journal de Crelle*, v. 127.

[8] Königsberger, "Uber den Eisensteinschen Sätz von der Irreductibilität algebraischer Gleichungen," *Journal für die Mathematik*, v. 115, p. 53-78, 1895.

[9] Kronecker, "Uber die Irreductibilität von Gleichungen," *Monatsberichte, Akademie der Wissenschaften Berlin*, p. 155-162, 1880.

[10] Lutz, Robert E. Jr, *An Implemented Transformational Scheme for Monic Polynomials with Integer Coefficients*, Masters Thesis, Naval Postgraduate School, Monterey, California, June 1971.

[11] Mann, Henry B., *Introduction to Algebraic Number Theory*, The Ohio University Press, 1955.

[12] MacLane, Saunders, "A Construction for Absolute Values in Polynomial Rings," *American Mathematical Society, Transactions*, v. 40, p. 363-395, 1936.

[13] MacLane, Saunders, "A Construction for Prime Ideals as Absolute Values of an Algebraic Field," *Duke Mathematics Journal*, v. 2, p. 492-510, 1936.

[14] MacLane, Saunders, "The Schönemann-Eisenstein Irreducibility Criteria in Terms of Prime Ideals," *American Mathematical Society, Transactions*, v. 43, p. 226-239, 1938.

[15] McCarthy, Paul J., *Algebraic Extension of Fields*, Blaisdell Publishing Company, 1966.

[16] Netto, "Uber die Irreductibilität ganzer ganzzahliger Functionen," *Mathematische Annalen*, v. 48, p.81-88, 1897.

[17] Perron, "Uber eine Anwendung der Idealtheorie auf die Fräge nach der Irreduzibilität algebraischer Gleichungen," *Mathematische Annalen*, v. 40, p. 448-458, 1905.

[18] Schönemann, "Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modul eine reale Primzahl ist," *Journal für die Mathematik*, v. 31, p. 296-235, 1845.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0212 Naval Postgraduate School Monterey, California 93940	2
3.	Department Chairman, Code 53 Department of Mathematics Naval Postgraduate School Monterey, California 93940	2
4.	Asst Professor D. L. Davis, Code 53 Dv (Thesis Advisor) Department of Mathematics Naval Postgraduate School Monterey, California 93940	2
5.	Capt. Edward C. Traasdahl, USMC 2341 Park Avenue Long Beach, California 90815	10

Thesis
T7674
c.1 Traasdahl
Irreducibility over
the rationals.
103224